HITACHI
Inspire the Next

Hitachi Command Suite

Automation Director

Installation and Configuration Guide

Hitachi Data Systems

MK-92HC204-02

Contents

Preface

This document describes how to install and configure Hitachi Automation Director (HAD).

Intended audience

This document provides instructions for storage administrators, who are responsible for storage, services, and applications within the storage environment.

Product version

This document revision applies to Hitachi Automation Director v8.1.4 or later.

Release notes

Read the release notes before installing and using this product. They may contain requirements or restrictions that are not fully described in this document or updates or corrections to this document.

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`
< > 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 KB	1,024 (2^{10}) bytes
1 MB	1,024 KB or $1,024^2$ bytes
1 GB	1,024 MB or $1,024^3$ bytes
1 TB	1,024 GB or $1,024^4$ bytes
1 PB	1,024 TB or $1,024^5$ bytes
1 EB	1,024 PB or $1,024^6$ bytes

Accessing product documentation

Product user documentation is available on the Hitachi Data Systems Portal: https://portal.hds.com. Check this site for the most current documentation, including important updates that may have been made after the release of the product.

Getting help

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

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

Overview

This chapter provides the following information:

- Product overview
- About related Hitachi Command Suite products
- Hitachi Automation Director system configuration
- Hitachi Automation Director installation and configuration workflow

Product overview

Hitachi Automation Director is a software solution that provides tools to automate and simplify the end-to-end storage provisioning process for storage and data center administrators. The building blocks of the product are pre-packaged automation templates known as Service Templates. These pre-configured templates are customized to your specific environment and processes for creating services that automate complex tasks such as resource provisioning. When configured, Automation Director integrates with existing Hitachi Command Suite applications to automate common infrastructure management tasks by utilizing your existing infrastructure services.

Automation Director includes the following features:

- Pre-configured service templates that help in creating automation services
- Automation services for intelligent provisioning of volumes from different storage classes
- Role-based access to defined services
- Performance-based pool selection that chooses the best performing pools from automation groups and provides pool information to each task for specifying the volume usage details
- Common service management attributes that can be assigned and shared across all automation services

About related Hitachi Command Suite products

Hitachi Automation Director is a part of Hitachi Command Suite, which includes the following components:

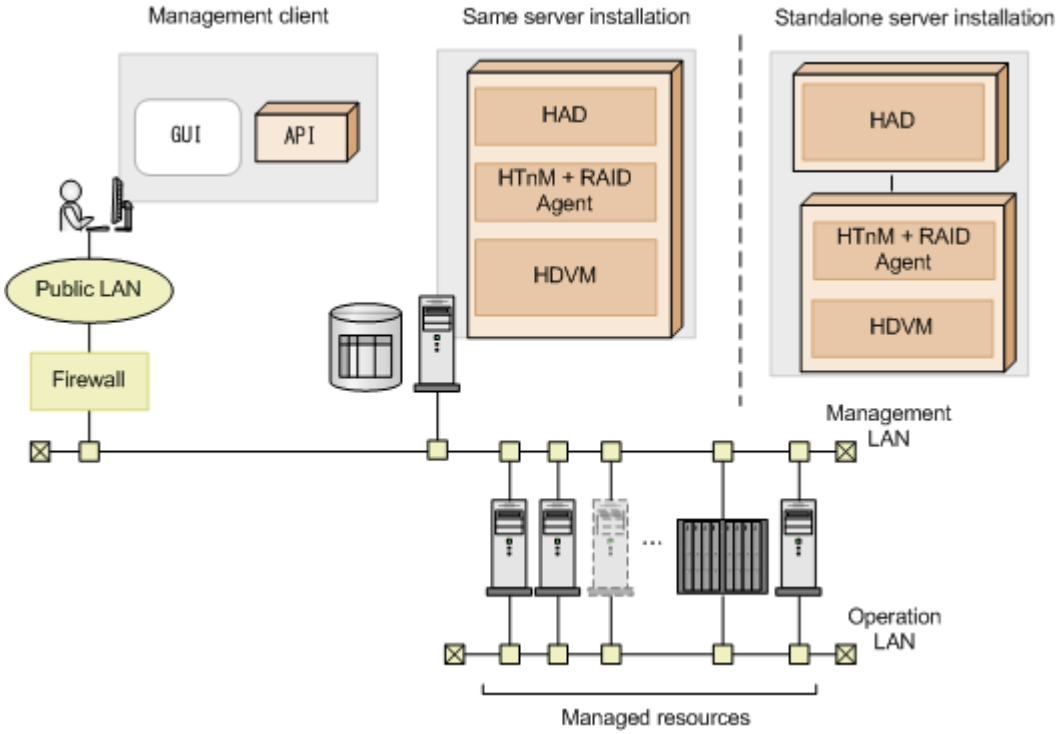
- Hitachi Device Manager
- Hitachi Tiered Storage Manager
- Hitachi Dynamic Link Manager
- Hitachi Replication Manager
- Hitachi Tuning Manager
- Hitachi Global Link Manager
- Hitachi Compute Systems Manager

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

Note: Only host information is synchronized when using both Automation Director and Device Manager, not information for other types of resources.

Hitachi Automation Director system configuration

There are two ways to set up your Hitachi Automation Director environment. The following figure shows the basic system configurations.



The basic system configuration environment can be set up as one of the following:

- Hitachi Automation Director is installed as a standalone product without any additional Hitachi Command Suite products.
- Hitachi Automation Director and Hitachi Device Manager (HDVM) are installed on the same server.

Note: You may also change from a same server configuration to a standalone setup by using the **`hcmds64prmset`** command. See Moving Command Suite Automation installation to a new host on page 54 for additional information.

Prerequisite Hitachi Command Suite products

The following table lists the supported Hitachi Command Suite products:

Product	Version
Hitachi Device Manager	8.1.1
Hitachi Tuning Manager*	8.1.1
Hitachi Replication Mananger**	8.1.4
* Tuning Manager is required only if you want to leverage Tuning Manager performance data to enable Automation Director to perform an intelligent selection of the pool when provisioning across a set of pools or arrays. ** Hitachi Replication Manager is required only if you use Thin Image services. If your configuration uses multiple Device Managers/Replication Managers, set up only one of the Replication Managers to run in Normal mode. The rest of the Replication Managers must always operate in Maintenance mode.	

Performance-based pool selection

You can use the performance-based pool selection of intelligent provisioning service. To enable the performance-based pool selection, check the settings of the following file.

Install location of HDvM\HicommandServer\config\tuningmanager.properties

This file contains properties for connecting to the Tuning Manager from the Device Manager.

If the Device Manager server and the Tuning Manager server are installed on the same machine, the system will run under the following settings:

- htnm.servers=1
- htnm.server.0.host=localhost
- htnm.server.0.protocol=http
- htnm.server.0.port=22015

For additional information, see the following sections in *Hitachi Command Suite Administrator Guide*, MK-90HC175:

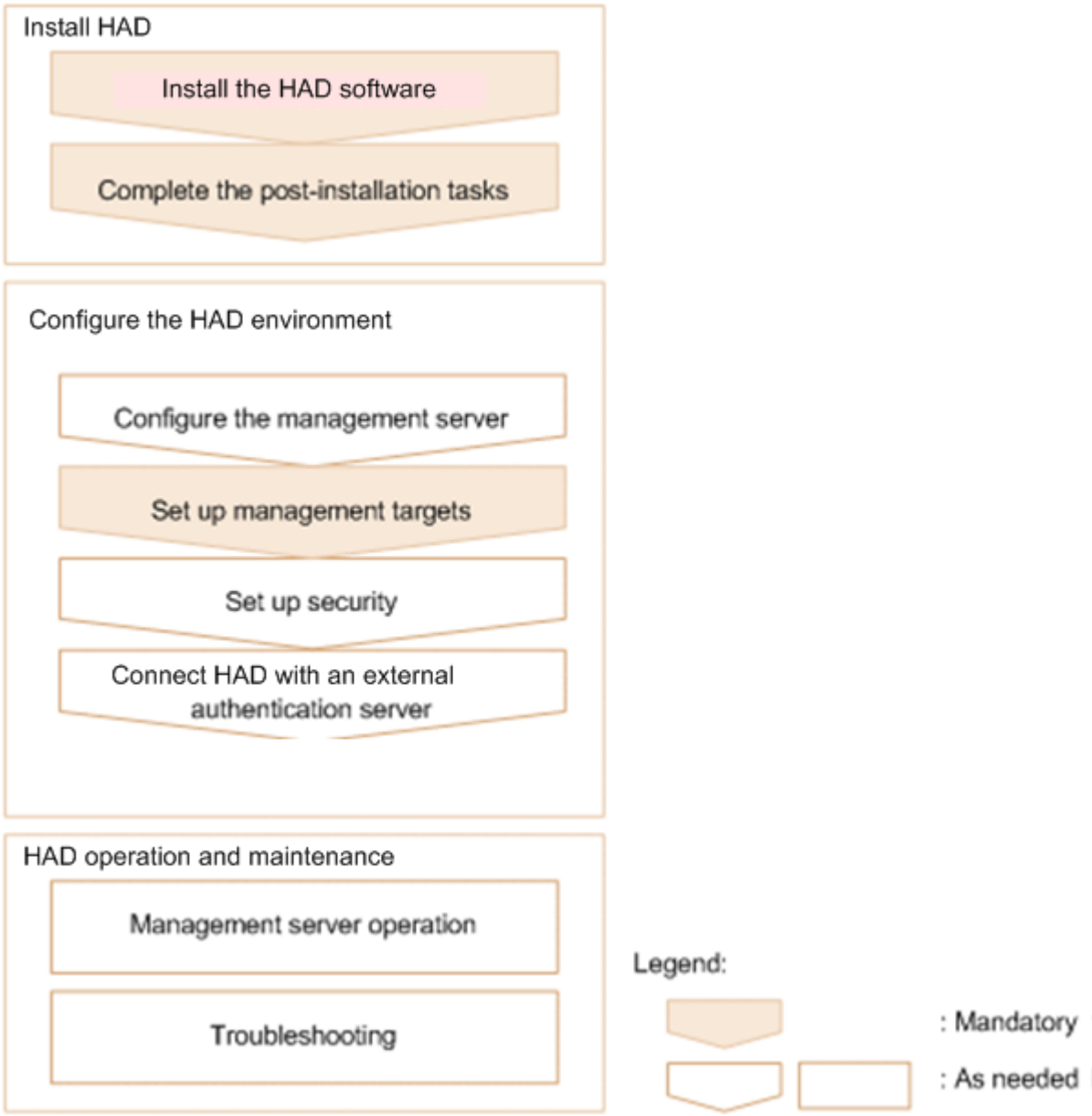
- Chapter 6, Configuring Device Manager for use with related products - Settings required to collect storage system performance information
- Appendix A, Device Manager server properties - Properties for connecting to Tuning Manager (`tuningmanager.properties` file)

Maximum number of Hitachi Device Manager servers supported by Automation Director

The maximum number HDvM servers that Automation Director can support is 50. For additional information see, Hitachi Command Suite System Requirements MK-92HC209.

Hitachi Automation Director installation and configuration workflow

The following figure illustrates an overview workflow, which includes installing and configuring Hitachi Automation Director.



This guide includes system installation, setup, management, and maintenance information. For details about using the management GUI to create, manage, and automate provisioning services, see the *Hitachi Command Suite Automation Director User Guide*.

2

Installing Hitachi Automation Director

This chapter describes how to install Hitachi Automation Director for Microsoft® Windows® in both cluster and non-cluster environments.

- ☐ Installation prerequisites
- ☐ Installing Hitachi Automation Director
- ☐ Installing Hitachi Automation Director in a cluster environment
- ☐ Post-installation tasks

Installation prerequisites

Perform the following tasks before installing Hitachi Automation Director:

- Verify that .NET Framework 3.5.1 is installed on the management server. To install it, follow the procedure for the operating system that is running on the management server. Before installing the .NET Framework, verify that the prerequisite version of IIS is installed on the server.
- Verify that the environment and the management server meet all hardware and software requirements. For details on the system requirements, see *Hitachi Command Suite System Requirements,* MK-92HC209. For details about hardware size and space requirements, see the Hitachi Command Suite Automation Director Release Notes.
- Ensure the ports used by Automation Director are available. Verify that the ports on the management server are not in use by other Hitachi Command Suite products and no conflicts exist. If a port is in use by another Hitachi Command Suite product, then neither product may operate correctly. See Port settings on page 78.
- Resolve the names for the related machines. See Name resolution on page 20.
- Ensure Windows administrator permissions are obtained to complete the installation and configuration tasks included in this guide.
- Disable any security monitoring, virus detection, or process monitoring software on the server.
- Close any Windows Services or open command prompts.
- If the server is running any other Hitachi Command Suite products, stop the services for those products.
- Make sure the server system time is correct. If Hitachi Command Suite is installed on a different server, synchronize the Automation Director server time with the Hitachi Command Suite server. For information about changing the server time, see Changing the server time on page 18.

Changing the server time

It is important to ensure the Automation Director server Operating System time setting is synchronized with the Hitachi Command Suite management server.

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

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

- Configure the settings so that the time is adjusted when the service discovers a time discrepancy.
- The service adjusts the time setting only as long as the time difference remains within a certain range. Based on the maximum range value, set the frequency so that the time difference never exceeds the fixed range.

An example of a service that can adjust the time as long as the time difference does not exceed a fixed range is the Windows Time service.

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

If you cannot use the functionality that adjusts the server time automatically, or if you want to manually change the system time, perform these steps:

1. Stop the Hitachi Command Suite Common Component and all Hitachi Command Suite product services, for example:
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO
   - HBase 64 Storage Mgmt SSO Service
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Comm Server
   - HiCommand Suite Tuning Manager
   - HiCommand Performance Reporter
   - HCS Tuning Manager REST Application
   - HAutomation Engine Web Service
   - Device Manager Server Service
   - Tiered Storage Manager Server
2. Record the current time of the management server, and then reset the time.
3. Determine when to restart the services.

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

Verify that the Automation Director management server reflects the correct time.

Changing the name resolution setting

If you install Automation Director and Hitachi Command Suite on two different machines, you must resolve the name of the Automation Director server that connects to the client.

You must also resolve the name of the machine where Automation Director is installed.

If you install Automation Director on the same machine as Hitachi Command Suite, you must resolve the names of the machine on which you want to run the browser to access Automation Director.

Update your configuration settings so that the system can resolve the IP address from the management server host name that is set as the `ServerName` property on the first line of the `user.httpsd.conf` file. To verify that the IP address resolves to the host name, run the following command:`ping` *`management-server-host-name`*.

Avoiding port conflicts

Before a new installation of Automation Director, verify that the ports that Automation Director will use on the management server are not in use by other products. If a port is being used by another product, neither product may operate correctly.

To ensure that the necessary ports are not in use, use the **`netstat`** command. See also Changing Automation Director port numbers on page 34 and Port settings on page 78.

Installing Hitachi Automation Director

If you are installing multiple Hitachi Command Suite products on a single management server, use the All-in-One installer to install multiple products simultaneously with minimal input or tasks. If you do not want to use the default installation parameters or if you want to install in a cluster environment, use the product installer from the integrated installation media.

For details about the All-in-One installer, refer to the Hitachi Command Suite Installation and Configuration Guide. This document describes how to install Hitachi Automation Director using the product installer from the integrated product media.

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

Procedure

1. Ensure that your system meets all management server prerequisites as listed in the pre-installation checklist.
2. Verify that .NET Framework 3.5 SP1 (3.5.1) is installed.
3. If the server is running any products that use the Hitachi Command Suite Common Component, stop the following services:
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO
   - HBase 64 Storage Mgmt SSOService
   - HCS Device Manager Web Service
   - HBase 64 Storage Mgmt Common Server
   - HiCommand Suite Tuning Manager
   - HiCommand Suite Performance Reporter
   - HCS Tuning Manager REST Application
   - HAutomation Engine Web Service
   - Device Manager Server Service
   - Tiered Storage Manager Server Service
4. Insert the installation media into the DVD drive.

   If you are using the integrated media DVD and the installation program window does not open, double-click `index.html`.
5. Start the installation wizard by selecting **Automation Director** in the installation program window, and then clicking **Install**.
6. Follow the on-screen prompts and specify the required information.

   In most cases, accept the default installation selections.

   The **Install Complete** window opens.
7. Click **Finish**.

Note:

- If Automation Director is installed in an environment in which SSL communication is enabled or in which the port number for Hitachi Command Suite Common Component has been changed, the graphical user interface might not start, even if the **After the installation finishes, start the Hitachi Command Suite GUI** check box is selected in the **Install Complete** window.
- If this problem occurs, check the changed management server information, and then enter the URL for Automation Director in the address bar of the web browser to start the interface.

Result

Automation Director is now installed.

Installing Hitachi Automation Director in a cluster environment

This module provides information about installing and configuring a new installation of Hitachi Automation Director in a cluster environment.

About using Automation Director in a cluster environment

When using Hitachi Automation Director, you can increase reliability by setting up a failover management server using Microsoft Windows Server Failover Clustering.

When you use Automation Director in a cluster environment, you designate one Automation Director server as the active node and another as the standby node as follows:

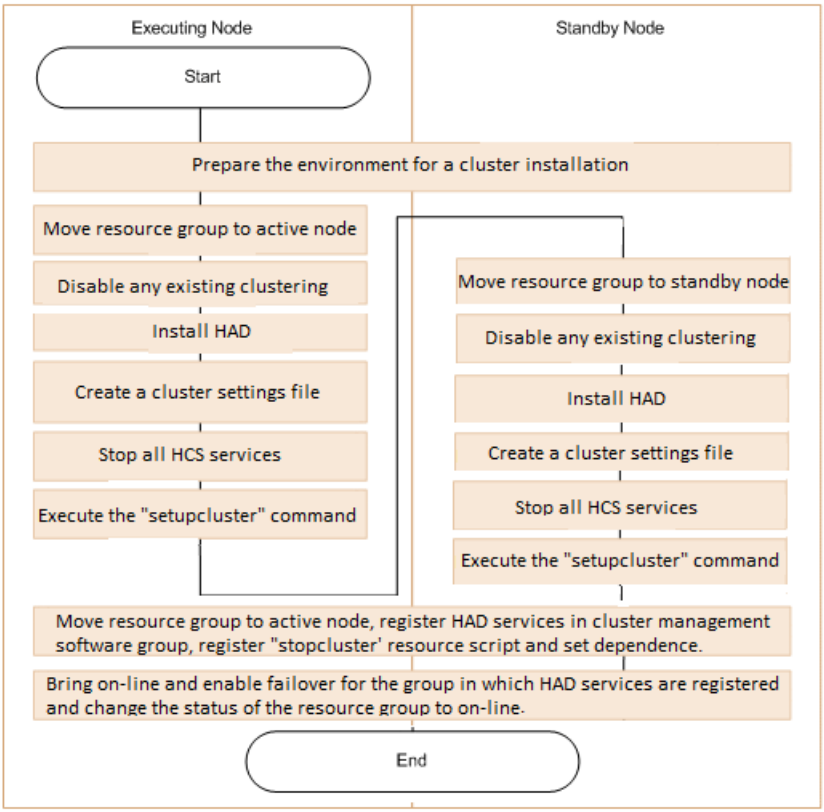
- Active node
  The active node is the host that is running services in a system that uses a cluster.
  If a failure occurs, the cluster services implements a failover, and the standby node takes over operation of the system resources so that there is no interruption of services.
- Standby node
  The standby node is the host that takes over operation of system resources from the active node if a failure occurs.

Note: If an active node fails over to the standby node, any tasks that are running fail and you must run the tasks again on the standby node.

Cluster installation workflow

When installing Hitachi Automation Director in a cluster configuration, you must follow a series of steps to prepare the executing node and standby nodes. Please see: Setting up HAD clustering on an active node on page 24 and Setting up HAD clustering on a standby node on page 26 for detailed instructions.

The following shows the general workflow for setting a up cluster environment:



Note: When installing Hitachi Automation Director to a cluster environment for the first time or when migrating from a non-cluster environment to a cluster environment, make sure that every node in the cluster has the same disk configuration, and all Hitachi Command Suite products are installed in the same location (including drive letter, path, etc.) on each node.

Note: When performing an upgrade of Hitachi Automation Director that has already been installed in a cluster configuration, you must disable the resource script before performing the updated installation.

Checking the cluster configuration using the cluster management software

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

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

- Check whether a group exists in which other Hitachi Command Suite product services are registered.

If a group in which Hitachi Command Suite services are registered already exists, use that group. Verify that the group consists only of resources related to Hitachi Command Suite products.
If no group in which Hitachi Command Suite services are registered exists, use the cluster management software to create a group in which you plan to register the Hitachi Automation Director services.

Note: Group names cannot contain the following characters: ! " % &) * ^ | ; = , < >

- Verify that the group in which you plan to register services includes the shared disk and client access point that can be inherited between the active and standby nodes. The client access point is the cluster management IP address and the logical host name.
- Verify that you can allocate, delete, and monitor resources by using the cluster management software without any issues.

Services that are used in a cluster environment can be failed over together by registering them as a group in the cluster management software. These groups might be referred to by different names, such as "resource groups" or "roles", depending on the versions of the cluster management software and the OS.

Setting up Hitachi Automation Director clustering on an active node

You can complete a new installation of Hitachi Automation Director on the management server on an active node in a cluster configuration.

Note: For instructions on setting up clustering on the standby node, see: Setting up a new HAD instance on an a standby node on page 26.

Procedure

1. Bring online the cluster management IP address and shared disk. Make sure that the resource group for the cluster installation is moved to the active node.
2. If you created the cluster environment using another Hitachi Command Suite product, use the following command to take offline and disable failover for the cluster group in which Hitachi Command Suite product services are registered:
   - From integrated installation media:
     integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
   - From the installation directory of a Hitachi Command Suite product with v8.1.4 or later:

HCS-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*

where

r - specifies the name of the group in which the Hitachi Command Suite product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".

3. Complete a new installation of Hitachi Automation Director on the active node.

   If another Hitachi Command Suite product already exists in the cluster environment, verify the following before installing Automation Director:

   - Specify the IP address of the logical host as the IP address of the management server.

   If no other Hitachi Command Suite products exist in the cluster environment, verify the following before installing Automation Director:

   - Specify the IP address of the active node as the IP address of the management server.

   Note: If you are upgrading Hitachi Automation Director in an environment that has already been set up in a cluster configuration, you need to prevent failover of the script that is registered to the resource group before performing the updated installation. In the cluster management software, right-click on the script which is registered to the resource group and, from the **[property]-[policy]** tab, set the resource so that it does not reboot.

4. Register the licenses for the products you plan to use. Access the IP address of the active node.
5. If you already have a Hitachi Command Suite product configured within the cluster, skip to the next step. If Automation Director is the first Hitachi Command Suite product in the cluster, do the following:

   a. Add the following information to a blank text file:

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

   Note: On an active node, you must specify `online` for `mode`.

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

6. Use the following command to ensure that the Hitachi Command Suite product services are stopped:
   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop/server AutomationWebService
7. Execute the **setupcluster /exportpath** ExportPath command where the ExportPath specifies the absolute or relative directory path.

Setting up Hitachi Automation Director clustering on a standby node

After setting up the clustering installation on an active node, you can complete installation of Hitachi Automation Director on the management server on a standby node in a cluster configuration.

Procedure

1. In the cluster management software, move the group containing the Hitachi Automation Director resources to the standby node by right-clicking the group, selecting **Move** and then selecting either **Select Node** or **Move this service or application to another node**.
2. If you created the cluster environment using another Hitachi Command Suite product, use the following command to take offline and disable failover for the cluster group in which Hitachi Command Suite product services are registered:
   - From integrated installation media:
     integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
   - From the installation directory of a Hitachi Command Suite product with v8.1.4 or later:
     HCS-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
     where
     r - specifies the name of the group in which the Hitachi Command Suite product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HCS cluster, you would specify "HCS cluster".
3. Complete a new installation of Hitachi Automation Director on the standby node.

   Before installing Hitachi Automation Director on the standby node, be aware of the following requirements:
   - You must install Hitachi Automation Director in the same location as on the active node.
   - If other Hitachi Command Suite products already exist and are active in the cluster environment, specify the logical host name (the virtual host name allocated to the cluster management IP address) as the IP address of the management server. If there are no other Hitachi

Command Suite products in the cluster environment, specify the IP address or the host name of the standby node.

Note: If you are upgrading Hitachi Automation Director in an environment that has already been set up in a cluster configuration, you need to prevent failover of the script that is registered to the resource group before performing the updated installation. In the cluster management software, right-click on the script which is registered to the resource group and, from the **[property]-[policy]** tab, set the resource so that it does not reboot.

4. Register the licenses for the products you plan to use.
5. If you already have a Hitachi Command Suite product configured within the cluster, skip to the next step. If Hitachi Automation Director is the first Hitachi Command Suite product in the cluster, do the following:
   a. Add the following information to a blank text file:

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

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

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

6. Use the following command to ensure that the Hitachi Command Suite product services are stopped:

   ```
   hcmds64srv /stop /server AutomationWebService
   ```

7. Execute the **`setupcluster /exportpath`** command where the `exportpath` specifies the absolute or relative directory path.

Registering the services and Initializing the cluster installation

After installing Hitachi Automation Director on the active and standby nodes in a cluster configuration, you can register the services and scripts then bring the clustering on line as described in the following steps:

Procedure

1. In the cluster management software, move the group containing the Hitachi Automation Director resources to the active node by right-clicking the group, selecting **Move** and then selecting either **Select Node** or **Move this service or application to another node**.

2. Register the Hitachi Automation Director services in the cluster management software group by using the following command:

   HCS-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvupdate /sreg /r *HCS-cluster-group-name* /sd *drive-letter-of-shared-disk* /ap *resource-name-for-client-access-point*

   where

   `r` - specifies the name of the group in which the Hitachi Command Suite product services including Hitachi Automation Director will be registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".

   `sd` - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Hitachi Command Suite products is divided into multiple shared disks, run the `hcmds64clustersrvupdate` command for each shared disk.

   `ap` - specifies the name of the resource for the client access point that is registered to the cluster management software.
3. Register the following as a script resource to execute the **`stopcluster`** command for the cluster software:
   - **`HAD-installation-folder\bin\stopcluster /prepare`**

   The script resource name and the script name are arbitrary. Configure the script so that the **`stopcluster`** command is executed only when the resource is offline. For more specific details, please consult the documentation for the cluster software you are using.

   Note: If you are upgrading Hitachi Automation Director, it is not necessary to register the script. However, you do need to enable failover of the script which is registered to the resource group. In the cluster management software, right-click and select the script which is registered to the resource group and then, from the **[property]-[policy]** tab, set the resource so that it reboots.

4. In the cluster management software, right click to select the resource script and set its dependence from the **[property]-[Dependencies]** tab. In addition, you must specify **[HAutomation Engine HCS-cluster-group-name]** to the resources that must be brought online before the script can be brought online.
5. On the active node, bring online and enable failover for the group in which Hitachi Command Suite services including Hitachi Automation Director are registered using the following command:

HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

where

r - specifies the name of the group in which the Hitachi Command Suite product services including Hitachi Automation Director are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".

6. Change the status of the resource group to **online** in the cluster software.

Post-installation tasks

Complete the following steps after installing Automation Director.

1. Confirm the registered URL (recommended).
2. Verify access to the Automation Director management server.
3. Register the license.
4. Change the System account password (recommended).
5. Set an email address for the System account.
6. Enable RMI communication.
7. Stop and restart HCS and HAD services (as needed).

Confirming the registered URL

Confirm the registered URL by using the following command:

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

Check the host name in URL. In case of non-cluster environment, the host name should be a physical host name. In case of the cluster environment, the host name should be a logical host name. If the registered URL is incorrect, change the URL by using the following command.

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

http://incorrect-IP-address-or-host-name:port-number

http://correct-IP-address-or-host-name:port-number

Verifying the installation

When installation is complete, verify that the installation was successful using a web browser.

Procedure

1. Open a web browser that is supported by Automation Director.
2. In the address bar, specify the URL for Automation Director in the following format:
   http://*HAD-server-address*:22015/Automation/

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

Registering a license

When you log on initially, you must specify a valid license key.

Procedure

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

Changing the System account password

The System account is a default account that has user management and execute permission for all Hitachi Command Suite products. When you install Automation Director for the first time, it is recommended that you change the System account password.

Procedure

1. From a management client, log on using the following credentials:
   - **User ID:** system
   - **Password (default):** manager
2. On the **Administration** tab, click **User Profile**.
3. Click **Change Password**, type the required passwords, and click **OK**.

Result

The default password is changed.

For details about changing user account passwords, see the *Hitachi Automation Director User Guide.*

Stopping and starting Hitachi Command Suite and Automation Director services

You can stop or start Hitachi Command Suite and Automation Director services from the command prompt. You can also stop or start Hitachi Command Suite from the Start Menu as well.

Note: You cannot start HAD services from the Start Menu.

Stopping and starting all services from the Start menu

The following procedure stops and starts all Hitachi Command Suite services:

Procedure

1. Select **Start > All Programs > Hitachi Command Suite > Manage Services**.
2. Click **Start - HCS** or **Stop - HCS**.

Stopping and starting all services from a command prompt

The following procedure stops and starts all Hitachi Command Suite and Automation Director services:

Procedure

1. At the command prompt, navigate to `C:\Program Files\HiCommand\Base64\bin`.
2. To stop the services, enter the following command:
   `hcmds64srv.exe /stop`
   To start services, enter the following command:
   `hcmds64srv.exe /start`

Stopping and starting only the Automation Director services from the command prompt

Procedure

1. Navigate to `C:\Program Files\HiCommand\Base64\bin`.
2. To stop services, enter the following command:
   `hcmds64srv.exe /stop /server AutomationWebService`
   To start services, enter the following command:
   `hcmds64srv.exe /start /server AutomationWebService`

Enabling RMI communication

You must configure RMI communication for Replication Manager before you can use HAD services. This step is required regardless of whether you are using Replication. If you do not enable RMI communication for Replication Manager, the Device Manager connections do not function properly and the connection status listed in the Administration Tab shows an error. See Enabling RMI communication for Replication Manager on page 52.

3

Configuring Automation Director

This chapter provides information on how to configure Automation Director.

Changing management server system settings

This module provides information about changing Automation Director management server system settings.

Changing Automation Director port numbers

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

Procedure

1. Stop Automation Director. See Stopping and starting Hitachi Command Suite and Automation Director services on page 30.
2. Edit the Automation Director properties.
   a. Open *Installation-folder-for-Hitachi-Command-Suite* `\Automation\conf\command_user.properties`.
   b. Change the value of `command.http.port` as required.
3. Start Automation Director. See Stopping and starting Hitachi Command Suite and Automation Director services on page 30.
4. If you changed the port that is used for communication between the management server and management clients (by default, 22015/TCP or 22016/TCP), change the URL for accessing Automation Director.

Changing the port number used by the task processing engine

If necessary, you can change the port number used by the Hitachi Automation Director task processing engine. The task processing engine is an internal component of Automation Director, which is responsible for running task processes. These separate processes require the use of communication ports.

Note: Before changing the port number, make sure that no tasks are running by checking the Status column on the Tasks tab in the Hitachi Automation Director GUI. Make sure that tasks in the In Progress, Waiting, Long Running status or processes that are stopped are not affected by the port number change.

Procedure

1. Stop Automation Director by running the **`hcmds64srv /stop`** command.
2. With a text editor, open the `%windir%\system32\drivers\etc\services` file, and change the value of the port number that is defined at `jp1ajs3cdinetd`.

3. In the *Automation-Director-installation-folder*\system\AJS3CD\conf\ directory, create a file named ajscd_DNA.properties and add the following entry:

   ajscd.port_number=*port-number-value-from-step-2*

4. Start Automation Director by running the **hcmds64srv /start** command.

Hitachi Command Suite property updates for port number changes

If you change Automation Director port numbers, you must update the Hitachi Command Suite Common Component properties that are listed in the following table:

Port number (default)	Property file path (HCS Common Component installation directory)	Location
22015/TCP	\uCPSB\httpsd\conf\user_httpsd.conf	Listen
		Listen [::]:
		#Listen 127.0.0.1:
22016/TCP	\uCPSB\httpsd\conf\user_httpsd.conf	*host-name*:*port-number* in the VirtualHost tag
		Listen
		Listen [::]:
22031/TCP	\uCPSB\httpsd\conf\user_hsso_httpsd.conf	Listen
22032/TCP	\HDB\CONF\emb\HiRDB.ini	PDNAMEPORT
	\HDB\CONF\pdsys	pd_name_port
	\database\work\def_pdsys	pd_name_port
22033/TCP	\uCPSB\CC\web\redirector\workers.properties	worker.HBase64StgMgmtSSOService.port
	\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\usrconf\usrconf.properties	webserver.connector.ajp13.port
22034/TCP	\uCPSB\CC\web\containers\HBase64StgMgmtSSOService\usrconf\usrconf.properties	webserver.shutdown.port

Changing the management server host name or IP address

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

Changing the management server host name

You can change the host name of the management server after installing Hitachi Automation Director.

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

Procedure

1. Make a note of the new management server host name and IP address.
   If you need to verify the host name on a Windows machine, use the `ipconfig /ALL` command to display the host name.
2. Back up Automation Director on the source host.
3. Change the host name of the management server. Then, restart the server.
4. Run `chgcommonbasehostname.bat` *`Revised host name`* to change the host name configuration of the common base.
5. Restore the backed-up data in the management server.
6. Stop Automation Director. See Stopping and starting Hitachi Command Suite and Automation Director services on page 30.
7. Edit the Hitachi Command Suite Common Component properties.
8. If you are running other Hitachi Command Suite products, revise the settings for those products as needed.
9. Verify that all Hitachi Command Suite services are running.
10. Run `chgenginehostname.bat` *`Revised host name`* to change the host name configuration of the automation engine.
11. If you use the old host name or IP address to access the management server from a browser, update the Hitachi Command Suite URL.
12. Run the `hcmds64srv /start` command to start Automation Director and verify that you can access the product using the new URL.

Result

The management server host name or IP address is changed.

Hitachi Command Suite property updates for management server host name changes

If you change the host name of the Automation Director management server, you must update the Hitachi Command Suite common properties that are listed in the following table:

Property file path (HCS Common Component installation directory)	Properties	Required changes
`\uCPSB\httpsd\conf\user_httpsd.conf`	`ServerName`	Change the value to the new host name.
	`VirtualHost` tag	If TLS or SSL is used for communication between the management server and management clients and a host name is specified, change the value to an asterisk (*).

Property file path (HCS Common Component installation directory)	Properties	Required changes
	`Servername` in the `VirtualHost` tag	If TLS or SSL is used for communication between the management server and management clients, change the value to the new host name.
`\HDB\CONF\pdsys` `\database\work\def_pdsys`	the `-x` option of `pdunit`	Change the value to the loopback address 127.0.0.1.
`\HDB\CONF\pdutsys` `\database\work\def_pdutsys`	`pd_hostname`	
`\HDB\CONF\emb\HiRDB.ini`	`PDHOST`	

Hitachi Command Suite property updates for management server IP address changes

If you change the IP address of the Automation Director management server, you must update the Hitachi Command Suite common properties that are listed in the following table:

Property file path (HCS Common Component installation directory)	Properties	Required changes
`\uCPSB\httpsd\conf` `\user_httpsd.conf`	`ServerName`	Change the value to the new host name or new IP address.
`\HDB\CONF\pdsys` `\database\work\def_pdsys`	the `-x` option of `pdunit`	If the old IP value is specified, change the value to the loopback address 127.0.0.1.
`\HDB\CONF\pdutsys` `\database\work\def_pdutsys`	`pd_hostname`	
`\HDB\CONF\emb\HiRDB.ini`	`PDHOST`	

Changing the Automation Director URL

This module provides information about changing the management server URL.

Changing the management server URL

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

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

Procedure

1. Verify the current URL using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64chgurl /list
2. If Automation Director is installed on a standalone server, change only the Automation Director URL using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64chgurl /change *new-URL* /type Automation
3. If Automation Director is installed on the same server, change all Hitachi Command Suite URLs that are running on this management server using the following command:

   HCS-Common-Component-installation-folder\bin\hcmds64chgurl /change *old-URL new-URL*
4. Change the URL for the shortcut file:
   - For Windows Server 2008 R2:
     Select **Start > All Programs > Hitachi Command Suite > Automation Director**, and then right-click **HAD Login**. Select **Properties**, and on the **Web Document** tab, change the URL.
   - For Windows Server 2012 and Windows Server 2012 R2:
     Select **Start > All apps > Hitachi Command Suite > Automation Director**, and then right-click **HAD Login**. Select **Properties**, and on the **Web Document** tab, change the URL.

   Use the following format for the URL:

   Protocol://*Management-server-IP-address-or-host-name*:*port-number*/Automation/login.htm

   Where:
   - *Protocol* is `http` for non-SSL communication and `https` for SSL communication.
   - *Management-server-IP-address-or-host-name* is the IP address or host name of the management server on which Hitachi Automation Director is installed.
   - *port-number* is the port number that is set for `Listen` line in the `user_httpsd.conf` file.
     For non-SSL communication, specify the port number for non-SSL communication (default: 22015).
     For SSL communication, specify the port number for SSL communication (default: 22016).
     The `user_httpsd.conf` file is in the *HCS-Common-Component-installation-folder*\uCPSB\httpsd\conf\ directory.

5. Verify that you can access Automation Director using the new URL.

Configuring secure communications

This module describes how to configure secure communications for Hitachi Automation Director.

About Automation Director security settings

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

Automation Director can use secure communications using SSL or TLS for the following types of communication:

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

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

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

Configuring secure communications for management clients

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

About secure communications for management clients

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

Setting up SSL on the server for secure client communication

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

Prerequisites

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

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

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

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

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

Procedure

1. Start Automation Director.
2. To create a private key (`httpsdkey.pem`), a certificate signing request (`httpsd.csr`), and a self-signed certificate (`httpsd.pem`) for the HCS Common Component, use the following command:

   ```
   HCS-Common-Component-installation-folder\bin
   \hcmds64ssltool /key HCS-Common-Component-installation-folder
   \uCPSB\httpsd\sslc\bin\demoCA\httpsdkey.pem /csr HCS-Common-
   Component-installation-folder\uCPSB\httpsd\sslc\bin\demoCA
   \httpsd.csr /cert HCS-Common-Component-installation-folder
   \uCPSB\httpsd\sslc\bin\demoCA\httpsd.pem /certtext HCS-
   Common-Component-installation-folder\uCPSB\httpsd\sslc\bin
   \demoCA\httpsd.txt /validity 365
   ```

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

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

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

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

3. When prompted, enter the following information after the colon(:).
   - Server Name (management server host name) - for example, HAD_SC1.
   - Organizational Unit (section) - for example, Automation Director.
   - Organization Name (company) - for example, Hitachi.
   - City or Locality Name - for example, Santa Clara.
   - State or Province Name (full name) - for example, California.
   - Country Name (2 letter code) - for example, US.

   To leave a field blank, type a period (.). To select a default value displayed within the brackets ([]), press **Enter**.
4. Send the certificate signing request (`httpsd.csr`) to the certificate authority to apply for a server certificate.

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

   The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.
5. Stop Automation Director.
6. Copy the private key (`httpsdkey.pem`) and the server certificate or the self-signed certificate (`httpsd.pem`) to the following directory:

   HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\ssl\server
7. Open the `user_httpsd.conf` file from the following location:

   HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf
8. Within the `user_httpsd.conf` file, do the following:

a. Uncomment the following lines by removing the hash [#] signs:

```
#Listen 22016

#<VirtualHost *:22016>
```

through

```
#</VirtualHost>
```

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

The following is an example of how to edit the `user_httpsd.conf` file:

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

b. Edit the following lines as required:

ServerName in the first line

ServerName in the <VirtualHost> tag

SSLCertificateKeyFile

SSLCertificateFile

#SSLCACertificateFile

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

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

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

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

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

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

Result

SSL is now implemented on the Automation Director server.

Closing the non-SSL communication port

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

Prerequisites

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

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

Procedure

1. Open `user_httpsd.conf`:

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

   ```
   :
   #Listen 22015
   #Listen [::]:22015
   #Listen 127.0.0.1:22015
   #SSLDisable
   :
   #<VirtualHost *:22016>
   # ServerName host-name
   :
   #</VirtualHost>
   ```
3. Run the following command to import the server certificate into the truststore (`jssecacerts`):

HCS-Common-Component-installation-folder\bin\hcmds64keytool -import -alias *unique-name-in-the-truststore* -file *HCS-Common-Component-installation-folder*\uCPSB\httpsd\conf\ssl\server*server-certificate-file* -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *password-to-access-the-truststore*

4. Verify the contents of the imported truststore.

   HCS-Common-Component-installation-folder\bin\hcmds64ssltool -list -v -keystore *HCS-Common-Component-installation-folder*\uCPSB\jdk\jre\lib\security\jssecacerts -storepass *truststore-password*
5. Restart Automation Director.
6. Verify that you can log on to the Automation Director user interface.

Setting up SSL on web-based management clients

To implement secure communications between the management server and management clients, you must set up SSL on all Automation Director management clients that access the Automation Director web-based user interface. You must first set up SSL on the management server before setting up the management clients. You are only required to follow this procedure the first time you access the management server from this client.

Prerequisites

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

Procedure

1. From the management web client, access the management server using an SSL connection by using the following URL:

   https://*HAD-management-server-name:port-number-for-SSL-communication*/Automation/
2. Install the SSL certificate.

Result

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

Setting up SSL on management clients running the CLI

To implement secure communication between the management server and management clients, you must set up SSL on all Automation Director management clients that access the server using the CLI. You must first set up SSL on the management server before setting up the management clients. You are only required to follow this procedure the first time you access the management server from this client.

Procedure

1. Save the Automation Director server certificate that is stored in the following directory to a temporary directory on the Automation Director CLI host.

   HCS-Common-Component-installation-folder\uCPSB\httpsd\conf\ssl\server

2. From a command prompt on the Automation Director CLI host, import the Automation Director server certificate to the truststore (cacerts) using the following command:

   jre-installation-folder\bin\keytool -importcert -trustcacerts -alias had -file *user-specified-folder**server-certificate-file* -keystore *jre-installation-folder*\lib\security\cacerts -storepass changeit

   where changeit is the default keystore password for the truststore (cacerts). If you receive an invalid password error, confirm the password with an administrator.

3. To set the Automation Director server location, use the following command:

   CLI-installation-folder\csm configure

4. When prompted, enter the following information:

   HAD server host name: *HAD-server-name*

   Use SSL: y

   HAD server port number: *port-number-for-SSL-communication*

Result

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

Configuring secure communications for managed servers

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

About secure communication for managed servers

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

There are no additional steps required to implement SSL/TLS secure communication for servers unless you want to improve communications security for alerts sent by the server. You can strengthen security by creating an additional self-signed certificate or obtaining a new server certificate from

a certificate authority. If you choose to use a new certificate, you must update the management server SSL information from the Automation Director user interface.

Strengthening security for managed server alert communication

To increase the level of security for alert communications sent from a Hitachi server (including an LPAR manager on a blade server), you can create a keystore and import a server certificate or a self-signed certificate. To further increase security, you can also import the certificate for a Hitachi server to the keystore of the management server.

Prerequisites

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

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

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

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

Procedure

1. Stop Automation Director.
2. Create a new keystore by using the following command:

   ```
   C:\Program Files\HiCommand\bin\hcmds64keytool -genkey -
   keystore C:\Program Files\HiCommand\Base64\uCPSB\jdk\jre\lib
   \security\jssecacerts\conf\ssl\keystore-file-name -storepass
   keystore-password -keypass secret-key-password -keyalg RSA -
   keysize 2048 -sigalg SHA256withRSA -validity valid-days-of-
   certificate -alias unique-name-in-keystore
   ```

3. If you want to use a self-signed certificate, go to step 7. If you want to use a server certificate issued by a certificate authority, use the following command to create a certificate signing request:

   ```
   C:\Program Files\HiCommand\bin\hcmds64keytool -certreq -file
   certificate-signing-request-file-name -keystore C:\Program
   Files\HiCommand\Base64\uCPSB\jdk\jre\lib\security\jssecacert
   \conf\ssl\keystore-file-name -storepass keystore-password -
   keypass secret-key-password -alias unique-name-in-keystore
   ```

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

   The server certificate issued by the certificate authority is usually sent by email. Ensure that you save the email and the server certificate sent by the certificate authority.
5. To import the certificate authority server certificate to the keystore, use the following command:

   ```
   C:\Program Files\HiCommand\bin\hcmds64keytool -import -file
   certificate-file-of-certificate-authority -keystore C:
   \Program Files\HiCommand\Base64\uCPSB\jdk\jre\lib\security
   \jssecacert\conf\ssl\keystore-file-name -storepass keystore-
   password -alias unique-name-in-keystore
   ```

   Note: Refer to the *Hitachi Command Suite Administrator Guide,* MK-90HC175 for additional information on the **`hcmds64keytool`** command. Be sure to also use the HDvM server certificate, which is the PEM format for the **`-file`** parameter.

6. To import the server certificate issues by the certificate authority to the keystore, run the following command:

   ```
   C:\Program Files\HiCommand\bin\hcmds64keytool -import -file
   server-certificate-file -keystore C:\Program Files\HiCommand
   \Base64\uCPSB\jdk\jre\lib\security\jssecacert\conf\ssl
   \keystore-file-name -storepass keystore-password -alias
   unique-name-in-keystore
   ```
7. To import the certificate for the Hitachi Server to the keystore, run the following command:

   ```
   C:\Program Files\HiCommand\bin\hcmds64keytool -import -file
   certificate-file-for-Hitachi-server -keystore C:\Program
   Files\HiCommand\Base64\uCPSB\jdk\jre\lib\security\jssecacert
   \conf\ssl\keystore-file-name -storepass keystore-password -
   alias unique-name-in-keystore
   ```
8. Open the `user.properties` file:

   ```
   HAD-installation-folder\HiCommand\conf\user.properties
   ```
9. For the `had.keystore.filename` property, specify the name of the keystore file that you created.
10. If you import a certificate for a Hitachi server in step 3, locate the `had.certification.verify` property and specify Enable. If you do not see the property in the file, add it.
11. If you migrate LPARs and want to enable encrypted communication only between the management server and the LPAR manager, specify Disable for the `hvm.lpar.migration.allow.plaintext` property. If you do not see the property in the file, add it.

12. Save the file and start Automation Director.
13. From a management client, log in to Automation Director and enable the new keystore. For details, see the *Automation Director User Guide*.

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

```
HCS-Common-Component-installation-folder\bin
\hcmds64keytool -exportcert -file certificate-file-to-
export -keystore HAD-installation-folder\HiCommand\conf
\ssl\keystore-file-name -storepass keystore-password -
alias unique-name-in-keystore
```

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

Result

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

About setting up secure communication for an external authentication server

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

Changing the port number of the authenticator connection for the primary HCS server

To change the port number:

Execute the **hcmds64prmset** command to change the port number of the authenticator connection as follows:

```
HCS-Common-Component-installation-folder\bin\hcmds64prmset /
hostname <the hostname of a primary server> /sslport <SSL port
number>
```

by:

- Specifying the same name as Common Name (CN) for the credentials as "hostname".
- Specifying the SSL port number (`sslport`) of a common component. The default is 22016.

Importing the server certificates of VMware vCenter

When using VMware service or the server certificates of VMware vCenter, you must import the truststore of a common component for Hitachi Command Suite.

You must also import the following certificates:

- certificate authority
- intermediate certificate authority
- route certificate authority

If the prominent certificate authority has already been imported, this operation is not necessary.

In Windows, use the **hcmds64keytool** command. For Unix, use standard **keytool**. To import the credentials in Java, the trust store password after a modification should specify six or more characters. In addition, you must ensure the new alias name does not conflict with an existing alias name.

For Windows:

```
HCS-Common-Component-installation-folder\bin\hcmds64keytool -
import -alias <alias name> -keystore <Hitachi Command Suite The
installation folder>\uCPSB
\jdk\jre\lib\security\jssecacerts -storepass <trust store
password> -file <certificate file>
```

For Unix:

```
HCS-Common-Component-installation-folder/uCPSB/jre/jdk/bin/
keytool  -import -alias <alias name> -keystore HCS-Common-
Component-installation-folder/uCPSB/jdk/jre/lib/security/
jssecacerts -storepass <trust store password> -file <certificate
file>
```

Additional guidelines

- For information on the security setting method of VMware vCenter, see the VMware documentation.
- To acquire the server credentials set as the vCenter server, refer to the VMware documentation for accessing server certificates.

Importing the server credentials to a Device Manager agent trust store

When using replication service, you must import the server certificates of Hitachi Device Manager at the Device Manager agent's trust store.

Refer to "Importing a server certificate into the truststore for the Device Manager agent" in the *Hitachi Command Suite Administrator Guide* for details.

Importing the server credentials of Device Manager to the trust store of an HCS common component

To communicate between the Hitachi Command Suite common components in a Device Manager server and Device Manage when using Replication service, you must import the server certificates of Device Manager, or the certificate of the certificate authority for the truststore of a Hitachi Command Suite common component.

Downloading the trust store file of Device Manager

When using a self-signed certificate, connect with either of the following uniform resource locators by a web browser, and download a trust store. This is not necessary when using the certificates of certificate authority.

- Internet-protocol one-plus-one address of a Device Manager server, or https:// <hostname>:<the SSL port number of a Device Manager server>/service/HiCommandCerts
- Internet-protocol one-plus-one address of a Device Manager server, or http:// <hostname>:<non-SSL port number of Device Manager server>/service/HiCommandCerts.

Note: A port number is set to SSL:2443 or non-SSL:2001 by default.

See "a build of a Hitachi Command Suite Software system-configuration guide SSL client" for details.

Exporting of a Device Manager self-signed certificates

When using a self-signed certificate, use the **`hcmds64keytool`** for exporting the server credentials of Device Manager from the downloaded trust store. This is not necessary when using the certificates of a certificate authority.

Note: Specify the downloaded trust store as a trust store file.

See "a build of a Hitachi Command Suite Software system-configuration guide SSL client" for details.

For Windows :

```
HCS-Common-Component-installation-folder\bin\hcmds64keytool -
export -keystore <trust store file> -alias <alias name> -file
<certificate file >
```

For Linux :

```
HCS-Common-Component-installation-directory/bin/hcmds64keytool -
export -keystore <trust store file> -alias <alias name> -file
<certificate file >
```

Importing the credentials of Device Manager to the trust store of a Hitachi Command Suite common component

Import the exported server certificates of a self-signature or the credentials of certificate authority at a trust store.

In Windows, use the **hcmds64keytool** command. For Unix, use the standard **keytool** command. To import the credentials in Java, the trust store password after a modification should specify six or more characters. In addition, you must ensure the new alias name does not conflict with an existing alias name.

When using the certificates provided by a certificate authority, the certificates of an intermediate certificate authority and route certificate authority which results to route certificate authority besides certificate authority needs to be imported. The prominent certificate authority may already be imported, in which case, this procedure is unnecessary.

You must also import the following credentials:

- certificate authority
- intermediate certificate authority
- route certificate authority

If the prominent certificate authority has already been imported, this operation is not necessary.

In the case of Windows :

```
HCS-Common-Component-installation-Folder\bin\hcmds64keytool -
import -alias <alias name> -keystore HCS-Common-Component-
installation-directory\uCPSB\jdk\jre\lib\security\jssecacerts -
storepass <trust store password> -file <certificate file>
```

In the case of Unix :

```
HCS-Common-Component-installation-directory/jdk/bin/keytool -
import -alias <alias name> -keystore
HCS-Common-Component-installation-directory/uCPSB/jdk/jre/lib/
security/jssecacerts -storepass <trust store password> -file
<certificate file>
```

Enabling RMI communication for Replication Manager

Enable RMI communication for Replication Manager on the management server as described in this section.

Operations to complete in advance

Log into the Device Manager server as a user with Administrator permissions (for Windows) or as a root user (for Linux).

To enable RMI communication for Replication Manager:

Procedure

1. Stop the services of Hitachi Command Suite product.
2. Specify `true` for the `base.rmi.enabled` property in the `base.properties` file of Replication Manager. The `base.properties` file is stored in the following location:

   In Windows:

   Installation-folder-for-Hitachi-Command-Suite
   `\ReplicationManager\conf`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `ReplicationManager/conf`

   For details on the `base.properties` file and the `base.rmi.enabled` property of Replication Manager, see the *Replication Manager Configuration Guide*.
3. Set up the `rpmlib.rpm.port` property in the `rpmlib.properties` file of the Device Manager server.

   Enter the port number that is set for the `base.rmi.port` property in the `base.properties` file of Replication Manager. If you did not change the value for the `base.rmi.port` property (default: 25200), this operation is unnecessary.

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

   In Windows:

   Installation-folder-for-Hitachi-Command-Suite
   `\ReplicationManager\conf`

   In Linux:

   installation-directory-for-Hitachi-Command-Suite/
   `ReplicationManager/conf`

   For details on the `base.properties` file and the base.rmi.enabled property of Replication Manager, see the *Replication Manager Configuration Guide*.
4. Start the services of Hitachi Command Suite product.
   See "Enabling RMI Communication for Replication Manager" in the *Hitachi Command Suite Administrator Guide* for additional information as required.

Moving a Hitachi Automation Director installation from one host to another

If necessary, you can relocate an installation of Hitachi Automation Director from one host to another.

Note: If the hostname or IP address of the replacement source and hostname or IP address of the replacement destination are different, perform the steps in Changing the management server host name or IP address on page 35.

Prerequisites

Make sure following settings are the same between the source host and the replacement destination host:

- The hostname and IP address.
- The character-code type.
- The account of the Operating System user used by Hitachi Automation Director
- The HCS product environment (configuration, version, and revision).
- The installation path of Automation Director.

You should also make sure that no tasks are currently being processed in the "Status" column of the **Tasks** tab of Hitachi Automation Director with the indication "In Progress", "Waiting for Response", "Abnormal Detection", "Long Running", or "Terminated".

Procedure

1. Log into the management server using Administrator privilege.
2. Perform a backup of Automation Director on the source host.
   a. Stop the current services by running the **`hcmds64srv /stop`** command.
   b. Run the **`backupsystem`** command to perform the backup.
3. Transfer the archived backup file to the replacement destination host.
4. Log on to the management server for the destination host.
5. Perform a restore of Hitachi Automation Director on the replacement destination host.
   a. Stop the services by running the **`hcmds64srv /stop`** command.
   b. Run the **`restoresystem`** command to restore the backup.
   c. Modify the appropriate settings in the following configuration files to match the environment of the restore destination:
      - External authentication server integration config file (`exauth.properties`).

- Security definition file (security.conf).
- Audit log definition file (auditlog.conf).
- Setting of changing port number (user_httpsd.conf).
- SSL environment build procedure (user_httpsd.conf).

These configuration files are located in the following directories:

- *Backup destination folder* \HBase\base\conf
- *Backup destination folder* \HBase\base\httpsd.conf

6. If the port number is changed, modify the necessary settings to reflect the new port number.
7. Restart the services by running the **hcmds64srv /start** command.

Running Automation Director without an external network configuration

To run Automation Director in an environment that uses a private, internal network you need to disable to the Authenticode signature function. Authenticode verifies the integrity of the software as it is being downloaded or transferred over a network. Windows runs with the Authenticode signature function by default.

In an environment that has no connection to an external network, it might take more than 20 seconds before the system is able to run a service plug-in.

To disable the Authenticode signature, you must reconfigure the Microsoft.NET framework.

Procedure

1. Use a text editor to open the following files:
   a. **<system-drive>:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet.config**
   b. **<system-drive>:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config**
2. Set **'generatePublisherEvidence enabled'** to false as shown below and save the file.

```
-----------------------------------------

<configuration>

<runtime>

<generatePublisherEvidence enabled="false"/>

</runtime>

</configuration>
```

Changing the system configuration through the properties file (config_user.properties)

The `conf_user.properties` file is the definition file for configuring various Hitachi Automation Director settings such as logs and tasks. Note that changing the properties file, restarts the Hitachi Automation Director engine web service.

You can change the following configuration properties through this file:

- Log file configuration (specify the number of logs to store).
- Task and history configuration (specify the number of tasks and task histories to store).
- Configuration regarding remote command execution (SSH/telnet port number)
- Configuration information for email notification.
- Configuration information regarding Service Builder.

Format

specification-key-name=setting

Installation folder

HAD-installation-folder\conf

Description

When editing the properties file, take note of the following:

- Lines that begin with # are treated as comments
- Blank lines are ignored
- The encoding is ISO 8859-1
- The contents are case sensitive
- To specify \ in a character string, it must be written \\.
- If an invalid value is entered for a setting, it is set to its default value, and message **KNAE02022-W** is output to the integrated trace log and public log
- If the same specification key is entered multiple times in a file, the last one that is specified will take effect

Settings in the properties file

Category	Key name	Setting	Values	Default values
Logs[1]	`logger.sysloglevel`	Specifies the threshold for event log output.	• 0: Output only when the output level of the message ID is 0 • 10: Output when the output level of the message ID is 0 or 10	0
	`logger.message.server.MaxBackupIndex`	Specifies the maximum number of log backup files for a server.	1 - 16	7
	`logger.message.server.MaxFileSize`	Specifies the maximum log file size (in KBs) for a server.	4 - 2097151	1024
	`logger.message.command.MaxBackupIndex`	Specifies the maximum number of log backup files for a command.	1 - 16	7
	`logger.message.command.MaxFileSize`	Specifies the maximum log file size (in KBs) for a command.	4 - 2097151	1024
	`logger.TA.MaxFileSize`	Specifies the maximum log file size (in KBs) for a task.	4 - 2097151	1024
Task management	`tasklist.autoarchive.taskRemainingPeriod`	Specifies the period (in days) for terminated tasks to remain in the task list.	1 - 90	7
	`tasklist.autoarchive.executeTime`	Specifies the time to run the automatic archiving task.	00:00:00 - 23:59:59	04:00:00
	`tasklist.autoarchive.maxTasks`	Specifies the maximum number of tasks to keep in the task list.	100 - 5000	5000

Category	Key name	Setting	Values	Default values
	tasklist.autodelete.maxHistories	Specifies the maximum number of history entries to retain.	100 - 30000	30000
Service management	packagemanager.extraPresets.maxFiles	Specified the maximum number of preset property definition files per 1 service template which can be placed in the extra preset folder.	5 - 100	5
Repeats	foreach.max_value	Specifies the maximum number of concurrent tasks that can be executed by the Repeated Execution Plug-in.	1 - 99	3
File transfer, general command execution, remote command	ssh.port.number	Specifies the SSH port number of the operation target device.	0 - 65535	22
	telnet.port.number	Specifies the Telnet port number of the operation target device.	0 - 65535	23
Remote file operation retry	plugin.remoteFileAccess.retry.times	Specifies the retry count of the command which operates the file run internally by the contents plug-in and file transfer plug-in. The interval of the retry is fixed as 100 ms. Even if the temporary file access error occurs, it may be successful by performing a retry. However, if the file access error is not recovered, it takes extra time to perform a retry until the end of the plug-in. Set this property in the environment where the file access error occurs even if there is no problem with the disk, etc.	0 - 100	0
Terminal connection	plugin.terminal.prompt.account	Specifies the regular expression used to detect the user ID waiting state.	1 - 1024	login|Login Name|

Category	Key name	Setting	Values	Default values
		If the standard output and standard error output match the specified regular expression, the terminal connect plug-in (Telnet is specified for the protocol) determines that a user ID must be entered, and then it enters a user ID.		Username| UserName
	plugin.terminal.prompt.password	Specifies the regular expression used to detect the password waiting state. If the standard output and standard error output match the specified regular expression, the terminal connect plug-in (Telnet is specified for the protocol) determines that a password must be entered, and then it enters a password.	1 - 1024	password| Password| PassWord
	telnet.connect.wait	Specifies the waiting time (in seconds) until the standard output is returned after an SSH connection is established with the operation target device.	1 - 600	60
Remote command	plugin.remoteCommand.executionDirectory.wmi	Specifies the path of the execution directory that contains the contents plug-in to run if the target host is running Windows. The execution directory must be created in advance. If the "Execution Mode" of the contents plug-in is "Script", the total string length of the specified value and the script file name do not exceed 140 characters. If the length exceeds 140 characters, transferring the script might fail. In addition, because the script file name must be specified in	0 - 256	

Category	Key name	Setting	Values	Default values
		90 characters or less, this value specified should be within 50 characters.		
	plugin.remoteCommand.executionDirectory.ssh	Specifies the path of the execution directory to execute the contents plug-in if the OS of the operation target host is UNIX. The execution directory is required to be created in advance.	0 - 128	
	plugin.remoteCommand.workDirectory.ssh	Specifies the working folder used when the file transfer plug-in or the contents plug-in is executed if the OS of the operation target host is UNIX. Enter a folder or a symbolic link as an absolute path (1 - 128 characters). In addition, the symbolic link can be included as the layer of the path.	1 - 128	/tmp/Hitachi_AO
Retry remote host connection	ssh.connect.retry.times	Specifies the number of retries in the event of a failed SSH connection to the operation target device.	0 - 100	3
	ssh.connect.retry.interval	Specifies the interval (in seconds) between retries in the event of a failed SSH connection to the operation target device.	1 - 600	10
	wmi.connect.retry.times	Specifies the number of retries in the event of a failed WMI connection to the operation target device.	0 - 100	3
	wmi.connect.retry.interval	Specifies the interval (in seconds) between retries	1 - 600	10

Category	Key name	Setting	Values	Default values
		in the event of a failed WMI connection to the operation target device.		
	telnet.connect.retry.times	Specifies the number of retries in the event of a failed Telnet connection to the operation target device.	0 - 100	3
	telnet.connect.retry.interval	Specifies the interval (in seconds) between retries in the event of a failed Telnet connection to the operation target device.	1 - 600	10
Retry email notification	mail.notify.retry.times	Specifies the number of retries in the event of a failure of the notification function to send an email.	0 - 100	3
	mail.notify.retry.interval	Specifies the interval (in seconds) between retries in the event of a failure of the notification function to send an email.	1 - 600	10
	mail.plugin.retry.times	Specifies the number of retries in case of failure to send email in the Email Notification Plugin.	0 - 100	3
	mail.plugin.retry.interval	Specifies the interval (in seconds) between retries in the event of a failure of the Email Notification Plugin to send an email.	1 - 600	10
Audit Log	logger.Audit.command.useLoginUserID	Specifies whether to output the HAD login user ID, in place of the user ID, to the subject identification information for the audit log when a command is executed.	true/false	false

Category	Key name	Setting	Values	Default values
Window refresh	client.events.refreshinterval	Specifies the refresh interval (in seconds) for events.	0 - 65535	5
Editor	client.editor.upload.maxfilesize	Specifies the maximum file size (in MB) that can be uploaded to the server from the terminal used for operating Automation Director by using the Editor window.	1 - 10	3
	client.editor.canvas.maxwidth	Specifies the maximum size (in px) of the width of Flow Editor view.	3600 - 10000	3600
	client.editor.canvas.maxhigh	Specifies the maximum size (in px) of the height of Flow Editor view.	2400 - 30000	2400
	server.editor.step.perTemplate.maxnum	Specifies the maximum number of steps per 1 service template.	320 - 40000	320
	server.editor.step.perLayer.maxnum	Specifies the maximum number of steps per 1 layer.	80 - 10000	80
	plugin.remoteFileAccess.retry.times			
	server.editor.publicProperty.perTemplate.maxnum			
	server.editor.propertyGroup.perTemplate.maxnum			
	server.longRunning.check.interval			

Category	Key name	Setting	Values	Default values
	server.longRunning.monitor.interval			

[1] The log output threshold for tasks can be set in Service Share Properties.

Example

logger.sysloglevel = 0

logger.message.server.MaxBackupIndex = 7

logger.message.server.MaxFileSize = 1024

logger.message.command.MaxBackupIndex = 7

logger.message.command.MaxFileSize = 1024

logger.TA.MaxFileSize = 1024

tasklist.autoarchive.taskRemainingPeriod = 7

tasklist.autoarchive.executeTime = 04:00:00

tasklist.autoarchive.maxTasks = 5000

tasklist.autodelete.maxHistories = 30000

mail.notify.retry.times = 3

mail.notify.retry.interval = 10

mail.plugin.retry.times = 3

mail.plugin.retry.interval = 10

client.events.refreshinterval = 5

Changing the port number for communicating with the HAD server through the command properties file (command_user.properties)

This is the definition file for setting the http port that is used when running commands. If you change the port number used for communications between Automation Director and the web browser, you must also change the http port used when executing commands to the same number. This is required for updating the definition file.

Format

specification-key-name=setting

Installation folder

HAD-installation-folder\conf

Description

One specification key and setting are specified per line. When editing the command properties file, take note of the following:

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- The encoding is ISO8859-1.
- The entries are case sensitive.
- To specify \ in a character string, it must be written \\.
- If an invalid value is entered for a setting, it is set to its default value, and message KNAE02022-W is output to the integrated trace log and public log.
- If the same specification key is entered multiple times in a file, the last one that is entered will take effect.

Setting

Key name	Setting	Values	Default value
command.http.port	Specifies the http port used when executing commands.	1–65535	22015

Example definitions

```
command.http.port = 22015
```

Changing the email notification definition

This is the definition file for email notification in the event of a failure or if an abnormality is detected in a task.

Format

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.hitachi.com/products/it/software/xml/
automation/conf/mailDefinition">
<title>email-title</title>
<body>email-body</body> </mail>
```

Installation folder

HAD-installation-folder\conf

Description

The definition file for email notification is in XML format. The locations to edit are the email-title and email-body sections.

When editing the file, take note of the following:

- A read error occurs if the definition file for email notification is missing, or is not well-formed XML. In this case, the email is sent with the default title and body.
- If you specify tags outside of <mail>, <title>, and <body>, even if the tags are well-formed XML, the tags and their content are ignored.
- An empty string will be specified for the value of a <title> or <body> tag that is omitted.
- The <mail> tag cannot be omitted. If it is omitted, the format is invalid and a read error occurs.
- The entries are case sensitive.

Settings in the definition file for email notification

Setting	XML element	Character string length	Default value
Title of email to be used in email notifications	<title>	Character string of 0-9,999 bytes	[HCS Automation] $TASK_NAME$ has changed to $TASK_STATUS$
Body of email to be used in email notifications	<body>	Character string of 0-9,999 bytes	Service Group Name: $SERVICE_GROUP_NAME$ Task Name: $TASK_NAME$ User Name: $USER_NAME$ Task Detail: $TASK_DETAIL_ URL$

XML entity references

Character you want in the email	Character string to be entered
&	&amp;
<	<
>	>

Character you want in the email	Character string to be entered
"	&quot;
'	&apos;

Embedded characters in the definition file for email notification

Embedded characters	Item	Remarks
$SERVICE_GROUP_NAME$	Service group name	Set to the character string representing the resource group name.
$TASK_NAME$	Task name	Set according to the format in the task properties.
$TASK_ID$	Task ID	
$TASK_KIND$	Task type	
$SERVICE_NAME$	Service name	
$TASK_TAGS$	Tag of the task	
$TASK_STATUS$	Task status	
$EXECUTION_DATE$	Date and time the operation was executed	
$PLANNED_START_DATE$	Planned date and time of start	
$START_DATE$	Actual date and time of start	
END_DATE	Date and time of end	
$USER_NAME$	User who executes the operation	
$TASK_DETAIL_URL$	URL of the Task Detail window	Set to a URL starting with http.

Changing the password policy through the security definition file (security.conf)

This is the definition file for settings related to user password conditions and locks. Users can modify the HCS password policy through this file to customize the security settings as required.

Format

specification-key-name=setting

Installation folder

Common-Component-installation-folder\conf\sec

Description

One specification key and setting are specified per line. The default state of the security definition file is as follows.

```
# This is the minimum length of the password
# (minimum: 1 -256 characters)
password.min.length=4

# This is the minimum number of uppercase characters included in
the password
# (minimum: 0-256 characters, character type: A-Z)
password.min.uppercase=0

# This is the minimum number of lowercase characters included in
the password
# (minimum: 0-256 characters, character type: a-z)
password.min.lowercase=0

# This is the minimum number of numeric characters included in
the password
# (minimum: 0-256 characters, character type: 0-9)
password.min.numeric=0

# This is the minimum number of symbolic characters included in
the password
# (minimum: 0-256 characters, character type: ! # $ % & ' ( ) * +
- . = @ \ ^ _ |)
password.min.symbol=0

# This specifies whether the user ID can be used for the password
# (true = cannot use the user ID, false = can use the user ID)
password.check.userID=false

# This is the minimum number of login failures before an account
is locked
# (minimum: 0-10 times)
account.lock.num=0
```

Settings

Key name	Setting	Settable values	Default value
password.min.length	Specifies the minimum number of characters in a password.	1 - 256	4

Key name	Setting	Settable values	Default value
password.min.uppercase	Specifies the minimum number of uppercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of uppercase letters.	0 - 256	0
password.min.lowercase	Specifies the minimum number of lowercase letters that must be included in the password. If 0 is specified, there are no constraints on the number of lowercase letters.	0 - 256	0
password.min.numeric	Specifies the minimum number of numeric characters that must be included in the password. If 0 is specified, there are no constraints on the number of numeric characters.	0 - 256	0
password.min.symbol	Specifies the minimum number of symbols that must be included in the password. If 0 is specified, there are no constraints on the number of symbols.	0 - 256	0
password.check.userID	Specifies whether or not to prevent the password from being the same as the user ID.	• true: prevent this • false: allow this	false
account.lock.num	Specifies the number of consecutive failed login attempts before the	0 - 10	0

Key name	Setting	Settable values	Default value
	account is automatically locked. If 0 is specified, the account is not automatically locked after failed login attempts.		

4

Removing Hitachi Automation Director

This chapter describes how to remove Hitachi Automation Director.

Removing Hitachi Automation Director

Perform the following steps to remove Hitachi Automation Director.

Prerequisites

- If tasks in the Status column of the **Tasks** tab of Hitachi Automation Director are in the Waiting, Waiting for Response, In Progress, "Long Running", or Failure Detection state, wait until the tasks have stopped or have finished running.
- Close all of the service dialog boxes.
- Close any Windows Services or open command prompts.
- Disable any security monitoring, virus detection, or process monitoring software on the server.

Caution: If other Hitachi Command Suite products are installed in the same host, do not delete the shared folder (`\Base\database`). Removing this folder will stop other Hitachi Command Suite products.

Procedure

1. Log on to Windows as the administrator.
2. Run the following command to stop all services:
   Common-Component-installation-folder`\bin\hcmds64srv /stop`
3. Open the **Control Panel**, and then choose **Programs and Features** or **Add or Remove Programs**.
4. Select **Automation Director**, and then click **Remove**, or select the program, right-click and select **Uninstall**.
5. In the **Setup** window, click **Uninstallation** to start the software removal process.
   The removal process deletes the *HAD-installation-folder*`\Automation` folder.

Result

Automation Director is removed from the host.

Removing Hitachi Automation Director software in a cluster environment

You can remove the Hitachi Automation Director software from the server in a cluster environment if you want to migrate to a different server or stop Hitachi Automation Director operation.

Note: If you remove Hitachi Automation Director, the properties files, log files, and other product-related files are deleted.

Procedure

1. In the cluster management software, move the group in which the Hitachi Automation Director services are registered from the standby node to the active node by right-clicking the group, and then selecting **Move** and then either **Select Node** or **Move this service or application to another node**.
2. Take offline and disable failover for the group in which Hitachi Command Suite services including Hitachi Automation Director are registered by using the following command:
   - From integrated installation media:
     integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*
   - From the installation directory of a Hitachi Command Suite product with v8.1.4 or later:
     Hitachi-Command-Suite-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvstate /soff /r *HCS-cluster-group-name*

     where

     r - specifies the name of the group in which the Hitachi Command Suite product services including Hitachi Automation Director are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".
3. Delete the Hitachi Command Suite services including Hitachi Automation Director by using the following command:

   Note: Before deleting the services, delete the "customer script" from the cluster management software.

   - From integrated installation media:
     integrated-installation-media\HCS\ClusterSetup\hcmds64clustersrvupdate /sdel /r *HCS-cluster-group-name*
   - From the installation directory of a Hitachi Command Suite product with v8.1.4 or later:
     Hitachi-Command-Suite-Common-Component-installation-directory\ClusterSetup\hcmds64clustersrvupdate /sdel /r *HCS-cluster-group-name*

     where

     r - specifies the name of the group in which the Hitachi Command Suite product services including Hitachi Automation Director are registered. If the group name contains spaces, you must enclose the

group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".

Note:

- All Hitachi Automation Director and Hitachi Command Suite product services that are registered in the group specified by the r option are deleted. However, the Hitachi File Services Manager services are not deleted.
- If you plan to continue using Hitachi Command Suite products, you can re-registered them after you remove Hitachi Automation Director. Deleting the Hitachi Automation Director services does not cause a problem.

  Remember that if you changed the service resource names, all resource names are reinitialized when the services are re-registered. Therefore, you must record the resource names for the services that you are deleting, and change the names after re-registering those services.

4. Delete the user script (the script that issues the "stopcluster /prepare" command) from the cluster software.
5. Use the following command to stop the Hitachi Command Suite products.

   HCS-Common-Component-installation-folder\bin\hcmds64srv /stop
6. Remove Hitachi Automation Director from the active node.
7. On the active node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
8. In the cluster management software, move the Hitachi Automation Director services group to the standby node by right-clicking the group, selecting **Move** and selecting either **Select Node** or **Move this service or application to another node**.
9. Remove Hitachi Automation Director from the standby node.
10. After performing the removal of the cluster installation, delete the Automation folder and, if you no longer plan to use any other HCS services, delete the Base folder as well from the standby node.
11. If the following resources are not in use by other applications, use the cluster management software to take them offline, and then delete them.
    - IP address
    - shared disk
12. On the standby node, delete any files and folders that are no longer required (such as those files and folders created during installation in the cluster environment).
13. If you want to continue using other Hitachi Command Suite products, use the following command to register the Hitachi Command Suite services in the cluster management software group:

HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvupdate /sreg /r *HCS-cluster-group-name* /sd *drive-letter-of-shared-disk* /ap *resource-name-for-client-access-point*

where

r - specifies the name of the group in which you to plan to register the Hitachi Command Suite product services. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".

sd - specifies the drive letter of the shared disk that is registered to the cluster management software. You cannot specify multiple drive letters for this option. If the database of Hitachi Command Suite products is divided into multiple shared disks, run the hcmds64clustersrvupdate command for each shared disk.

ap - specifies the name of the resource for the client access point that is registered to the cluster management software.

14. If you want to continue using other Hitachi Command Suite products, use the following command to bring online and enable failover for the group in which the Hitachi Command Suite services are registered:

    HCS-Common-Component-installation-folder\ClusterSetup\hcmds64clustersrvstate /son /r *HCS-cluster-group-name*

    where

    r - specifies the name of the group in which the Hitachi Command Suite product services are registered. If the group name contains spaces, you must enclose the group name in quotation marks ("); for example, if the group name is HAD cluster, you would specify "HAD cluster".

15. In the cluster management software, move the group containing the Hitachi Command Suite resources to the active node by right-clicking the group, selecting **Move** and then selecting either **Select Node** or **Move this service or application to another node**.

Deleting authentication data

If the KNAE04574-E warning dialog box appears even though the removal completes successfully, the deletion of authentication data has failed. Delete the authentication data by executing the hcmds64intg command on the server that administrates user accounts (on the host which Device Manager is installed in, and is connected to).

To execute the hcmds64intg command to delete the authentication data from a Windows host:

Procedure

1. Start all installed services of Hitachi Command Suite products by executing the following command:
   `Common-Component-installation-folder\bin\hcmds64srv /start`
2. Delete the authentication data by executing the following command:

   Common-Component-installation-folder`\bin\hcmds64intg /delete /type` *component-name* `/user` *user-ID* `/pass` *password*

   - `/type`
     Specify the name of the component that you want to delete. `Automation` can be specified.

   - `/user`
     Specify the user ID of a user who has the Admin (user management) permission. If you execute the command without the user option, you will be prompted to specify a user ID.
   - `/pass`
     Specify the password of a user who has the Admin (user management) permission. If you execute the command without the pass option, you will be prompted to specify a password.

Note: If you display a GUI window of another Hitachi Command Suite product without deleting the authentication data, the following problems might occur even after removing the Automation server:

- User management information of the Automation server is displayed.
- The button used to start the Automation server is enabled on the dashboard. Clicking the enabled button causes a link error to appear.

A

Hitachi Automation Director file location and ports

This appendix includes all the folders that are created as a part of Hitachi Automation Director installation.

Automation Director file location

Installation folders

The table lists the folders that are created when Hitachi Automation Director is installed. The Folder Details column lists default paths that can be changed during installation.

Folder locations	Folder details
Installation folder	*system-drive*\Program Files\HiCommand\Automation
Commands files	*system-drive*\Program Files\HiCommand\Automation\bin
Configuration files	*system-drive*\Program Files\HiCommand\Automation\conf
Folder for service templates	*system-drive*\Program Files\HiCommand\Automation \contents
Data files	*system-drive*\Program Files\HiCommand\Automation\data
Help files	*system-drive*\Program Files\HiCommand\Automation \docroot
Preset property definition files	*system-drive*\Program Files\HiCommand\Automation \extra_presets
Temporary working folder for installation and removal	*system-drive*\Program Files\HiCommand\Automation\inst
Library files	*system-drive*\Program Files\HiCommand\Automation\lib
Log files	*system-drive*\Program Files\HiCommand\Automation\logs
Source files for open source software	*system-drive*\Program Files\HiCommand\Automation \ossSource
System files	*system-drive*\Program Files\HiCommand\Automation \system
Working used by Internal command	*system-drive*\Program Files\HiCommand\Automation \webapps
Working folder	*system-drive*\Program Files\HiCommand\Automation\work
Common component	*system-drive*\Program Files\HiCommand\Base64

Port settings

Hitachi Automation Director uses the following port settings:

External connection port

Port number	Firewall	Description
22/tcp	HAD <--> Operation target	Used for SSH.

Port number	Firewall	Description
		cjstartweb uses this port.
23/tcp	HAD <--> Operation target	Used for Telnet. cjstartweb uses this port.
445/tcp or udp	HAD <--> Operation target	Used in shared management. cjstartweb uses this port.
135/tcp and 139/tcp	HAD <--> Operation target	Used in shared management. cjstartweb uses this port.
22015/tcp	Browser -> HAD	Use to access HBase Storage Mgmt Web Service. In non-SSL (unsecured) communication, initial setup is a required. This port number can be changed. `httpsd` uses this port.
22016/tcp	Browser -> HAD	Use to access HBase Storage Mgmt Web Service. In SSL (secured) communication, a setting is required. This port number can be changed. httpsd uses this port.
25/tcp	HAD -> SMTP server	Use for mail transmission. This port number can be changed. `cjstartweb` uses this port.
88/tcp or udp	HAD -> Kerberos server	`cjstartweb` uses this port.
359/tcp	HAD -> LDAP directory server	Use for `ldap/tls`. `cjstartweb` uses this port.
636/tcp	HAD -> LDAP directory server	Use for LDAPs. This port number can be changed. `cjstartweb` uses this port.
1812/udp	HAD -> Radius server	`cjstartweb` uses this port.

Internal connection port

Note: These ports are "reserved" and are used only for internal port connections.

Port number	Firewall	Description
20245/tcp	Task processing engine <--> Task processing engine	Use for manager's job status notification. `jp1ajs2report` uses this port.
20250/tcp	HAD → Task processing engine	Task processing engine uses this port. ajscdinetd uses this port. HAD always uses this port.
23031/tcp	HAD -> HAD	Use to access the following services: - HBase Storage Mgmt Web SSO Service - HSSO-dedicated Web server `cjstartweb` uses this port.
23160/tcp	Jobnet connector execution host <--> Jobnet execution host at the connection execution	Use for communication between scheduler services. `jp1ajs2gw` uses this port.
23800/tcp	Task processing engine <--> Task processing engine	Used in task processing engine's embedded database in a cluster configuration. `EmbeddedEdition_JF1` uses this port.

B

Using the hcmds64keytool utility

You can use the `hcmds64keytool` utility in a number of ways as follows:

- Importing a certificate into the truststore
- Removing a certificate from the truststore
- Exporting a Device Manager server self-signed certificate
- Specifying a unique name in the truststore, the truststore file name, and the password
- Checking the certificates imported into the truststore

Note: This operation helps to verify that a certificate was correctly imported.

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

Index

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-92HC204-02