HITACHI
Inspire the Next

JP1 Version 12

JP1/Automatic Operation Configuration Guide

3021-3-D03-40(E)

Notices

■ Relevant program products

- P-2A2C-E1CL JP1/Automatic Operation 12-60 (for Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022)

  The above product includes the following:
  - P-CC2A2C-EACL JP1/Automatic Operation - Server 12-60 (for Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022)
  - P-CC2A2C-EBCL JP1/Automatic Operation - Contents 12-60 (for Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022)
- P-2A2C-E3CL JP1/Automatic Operation Content Pack 12-60 (for Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022)
- P-822C-E1CL JP1/Automatic Operation 12-60 (for Red Hat Enterprise Linux 6 (x64), Red Hat Enterprise Linux 7, Oracle Linux 6 (x64), Oracle Linux 7, CentOS 6 (x64), CentOS 7, SUSE Linux 12)

  The above product includes the following:
  - P-CC822C-EACL JP1/Automatic Operation - Server 12-60 (for Red Hat Enterprise Linux 6 (x64), Red Hat Enterprise Linux 7, Oracle Linux 6 (x64), Oracle Linux 7, CentOS 6 (x64), CentOS 7, SUSE Linux 12)
  - P-CC822C-EBCL JP1/Automatic Operation - Contents 12-60 (for Red Hat Enterprise Linux 6 (x64), Red Hat Enterprise Linux 7, Oracle Linux 6 (x64), Oracle Linux 7, CentOS 6 (x64), CentOS 7, SUSE Linux 12)
- P-862C-E1CL JP1/Automatic Operation 12-60 (for Red Hat Enterprise Linux 8, Oracle Linux 8, CentOS 8)

  The above product includes the following:
  - P-CC862C-EACL JP1/Automatic Operation - Server 12-60 (for Red Hat Enterprise Linux 8, Oracle Linux 8, CentOS 8)
  - P-CC822C-EBCL JP1/Automatic Operation - Contents 12-60 (for Red Hat Enterprise Linux 8, Oracle Linux 8, CentOS 8)
- P-822C-E3CL JP1/Automatic Operation Content Pack 12-60 (for Red Hat Enterprise Linux 6 (x64), Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 8, Oracle Linux 6 (x64), Oracle Linux 7, Oracle Linux 8, CentOS 6 (x64), CentOS 7, CentOS 8, SUSE Linux 12)

■ Trademarks

RSA and BSAFE are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

JP1/Automatic Operation includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This product includes software developed by the University of California, Berkeley and its contributors.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England. The original software is available from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (http://www.modssl.org/).

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com)

4. This product includes the OpenSSL Toolkit software used under OpenSSL License and Original SSLeay License. OpenSSL License and Original SSLeay License are as follow:

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of

the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style

Open Source licenses. In case of any license issues related to OpenSSL

please contact openssl-core@openssl.org.

OpenSSL License

/* ==

* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

*

* 1. Redistributions of source code must retain the above copyright

* notice, this list of conditions and the following disclaimer.

*

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in

* the documentation and/or other materials provided with the

* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by IAIK of Graz University of Technology.

This product includes software developed by Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

This product includes software developed by the Java Apache Project for use in the Apache JServ servlet engine project (http://java.apache.org/).

This product includes software developed by Andy Clark.

Java is a registered trademark of Oracle and/or its affiliates.

HITACHI
Inspire the Next
Hitachi, Ltd.

Java COMPATIBLE ENTERPRISE EDITION

Java COMPATIBLE

RSA SECURED

Other company and product names mentioned in this document may be the trademarks of their respective owners.

■ Issued

Mar. 2022: 3021-3-D03-40(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-D03-40(E)) and product changes related to this manual.

Changes	Location
Windows Server 2022 was added as a supported operating system.	-
Notes were added regarding the use of products that use the same Common Component.	1.2.1, 1.3.1, 4.3.1, 4.3.2
The import of the service template provided by JP1/AO - Contents was added to the installation procedure.	1.3.1
The description of the files to be copied was changed.	1.4
Notes were added to the procedure for enabling the HTTPS connection between a web browser and JP1/AO.	1.6.3
The following operating systems are now supported: • Red Hat Enterprise Linux 8 • Oracle Linux 8 • CentOS 8	1.6.4, 1.8, 3.2.8, 4.3.1, 4.3.2, 4.5.1, 5.2, 6.3, 6.6.1
The format of the private key was added to the tips in the procedure for creating public and private keys.	1.7.4
The following items were added as setting items in the user-specified properties file (config_user.properties): • plugin.adapter.timeout • task.periodicalTaskArchive.enable • task.periodicalTaskArchive.period • task.periodicalTaskArchive.taskCountThreshold • task.periodicalTaskArchive.taskCountAfterArchive • task.execute.skip.serverStart • plugin.wmi.win32.UACAdministratorsExec • plugin.wmi.win32.CreationFlags.CREATE_NO_WINDOW	2.2
Descriptions of the following items, as setting items in the connection-destination property file, were changed: • wmi.workDirectory.sharedName • wmi.adapter.id	2.6
The following items were added as setting items in the connection-destination property file: • wmi.win32.UACAdministratorsExec • wmi.win32.CreationFlags.CREATE_NO_WINDOW	2.6
The encryption method for connecting to the LDAP directory server was added.	2.8, 3.2.3
Changes were made to the procedure (when the JP1/AO server is using Linux) for configuring settings to automatically start the JP1/AO service at the startup of the OS.	2.9

Changes	Location
A security configuration operation was added to the flow of tasks for linking with Active Directory.	3.2.1
Descriptions of security settings for communication with the LDAP directory server were added.	3.2.8
Descriptions of the definition files used for linking with JP1/IM were changed.	3.3.2
Task confirmation was added to the procedure for changing the host name of the JP1/AO server.	4.3.1
Notes on changing port numbers were added.	4.5.1
The procedure for changing a port number was added.	4.5.3, 4.5.4
The procedure for performing an overwrite or upgrade installation was changed.	6.3
The procedure for enabling failover of a resource group was changed.	6.5.5
The procedure for changing resource settings was changed.	6.6.5
The procedure for performing an overwrite installation of JP1/AO Content Pack was changed.	6.7
A description of how to prepare for uninstallation was added.	7.2
The prerequisite conditions for replacing a JP1/AO system were changed.	8.1, 8.2

In addition to the above changes, minor editorial corrections were made.

Preface

This manual describes how to set up JP1/Automatic Operation. In this manual, JP1/Automatic Operation is abbreviated to *JP1/AO*.

For reference information on JP1/AO manuals and a glossary, see the manual*JP1/Automatic Operation Overview and System Design Guide*.

■ Intended readers

This manual is intended for:

- Users who intend to set up a JP1/AO system
- Users who want to know how to set up, perform an overwrite or upgrade installation of, or uninstall JP1/AO, or who want to know how to migrate JP1/AO to a different environment

■ Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation	Full name or meaning
Active Directory	Microsoft(R) Active Directory
Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter
	Microsoft(R) Windows Server(R) 2012 Standard
Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
	Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
	Microsoft(R) Windows Server(R) 2019 Standard
Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter
	Microsoft(R) Windows Server(R) 2022 Standard

Windows is often used generically to refer to Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, or Windows Server 2012.

■ Formatting conventions used in this manual

The following describes the formatting conventions used in this manual.

Text formatting	Description
Character string	Italic characters indicate a variable. Example: A date is specified in *YYYYMMDD* format.

Text formatting	Description
Bold - **Bold**	Indicates selecting menu items in succession. Example: Select **File** - **New**. This example means that you select **New** from the **File** menu.
key+**key**	Indicates pressing keys on the keyboard at the same time. Example: **Ctrl**+**Alt** + **Delete** means pressing the **Ctrl**, **Alt**, and **Delete** keys at the same time.

■ Representation of JP1/AO-related installation folders

In this manual, the default installation folders for the Windows version of JP1/AO are represented as follows:

JP1/AO installation folder:

system-drive\Program Files\Hitachi\JP1AO

Common Component installation folder:

system-drive\Program Files\Hitachi\HiCommand\Base64

The installation folders for the Linux version of JP1/AO are as follows:

JP1/AO installation folder:

- /opt/jp1ao/
- /var/opt/jp1ao/

Common Component installation folder:

/opt/HiCommand/Base64

■ Diagrams of windows in the manual

Some windows in this manual might differ from the windows of your product because of improvements made without prior notice.

Contents

1 New Installation

This chapter explains how to perform a new installation of JP1/AO.

1.1 New installation procedure

After checking the prerequisites, install JP1/AO from the distribution media.

The following table describes the procedure for a new installation.

Table 1-1: New installation procedure

Task		Required/ optional	Reference
1	Check the installation prerequisites.	Required	1.2.1 Checking installation prerequisites
2	If the JP1/AO server OS is Linux 8, verify that the ports that JP1/AO will use are not in use.	Required	1.2.3 Check the port to use
3	Perform a new installation of JP1/AO from the distribution media.	Required	1.3.1 Procedure to perform a new installation of JP1/AO
4	Install the manual on the JP1/AO server.	Optional	1.4 Procedure to install the manual
5	Install JP1/AO Content Pack.	Optional	1.5.1 Procedure to install JP1/AO Content Pack
6	Enable HTTPS connections between Web browsers and JP1/AO servers.	Optional	1.6 Procedure to enable HTTPS connections between Web browsers and JP1/AO
7	Enable SSH connections with operation target devices.	Optional	1.7 SSH connections with operation target devices

1.2 Pre-installation tasks

1.2.1 Checking installation prerequisites

Prior to installing JP1/AO, you must check and prepare the installation environment.

About the JP1/AO server (server on which JP1/AO is to be installed)

- Log in to the JP1/AO server as a user with administrator or root permissions, and then perform the following operations:
  - Confirm that you have the correct version of JP1/AO for the OS you are running and that there is enough disk space to install JP1/AO.

    For details, see the *Release Notes*.
  - Confirm that the network environment uses the TCP/IP protocol.
  - Make sure that network sending and receiving are not blocked on the local host.

    The JP1/AO server cannot be installed or used in an environment where network sending and receiving are blocked for the IP address `127.0.0.1` on the local host. Do not block this communication in your firewall settings or in any other settings.
- Check the language (locale) settings of the JP1/AO server OS.

  JP1/AO supports the following language versions of OSs. One of the following languages must be set in the JP1/AO server OS.
  - Japanese
  - English
  - Chinese
  - German
  - French
  - Spanish
  - Korean
  - Russian

About the products other than JP1/AO

- Before you start the installation of JP1/AO, uninstall the following products that are not compatible with JP1/AO:
  - Hitachi Automation Director
  - Hitachi Ops Center Automator
- If JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products are installed, stop all JP1/OA, Hitachi Command Suite product, and Hitachi Ops Center product services.

  If JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products are installed on the JP1/AO server, they share the use of Common Component with JP1/AO. Before you install JP1/AO, all JP1/OA, Hitachi Command Suite products, and Hitachi Ops Center products must be stopped. Similarly, if you want to install JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products on the JP1/AO server, the JP1/AO service must be stopped.

About the tasks performed on the JP1/AO server

- Stop any security monitoring software, virus detection software, or process monitoring software.

  If such software is running, installation might fail.
- When installing JP1/AO in Windows, a service related to JP1/AO cannot start if **Startup Type** for that service is set to **Disabled**, which causes installation to fail. Make sure that **Startup Type** for each service is set to **Automatic** or **Manual**.

  For details about the relevant services, see the information about JP1/AO services in the *JP1/AO Administration Guide*.
- If the OS of the JP1/AO server is Linux, exceptions are not automatically registered in the firewall during an installation. Follow the procedure that is determined by the OS to register exceptions.
- If the Windows event log is being used by another program, do the following:
  - If the **Event Viewer** window is open, close it.
  - If the **Computer Management** window is open, close it.
  - Stop the event log monitoring program.

  If a program that references the event log is running during installation, the installation might fail.
- If the OS of the JP1/AO server is Windows, close any open command prompts before running the installation.

  If you do not close the command prompts before installing, the environment variable settings that you set during installation will not be applied.

Related topics

- 1.2.2 Language settings in the JP1/AO server OS
- JP1/AO services in the JP1/Automatic Operation Administration Guide
- Functions for linking with other products in the JP1/Automatic Operation Overview and System Design Guide
- Resident processes of Hitachi Command Suite in the Hitachi Command Suite Administrator Guide
- Lists of port numbers in the JP1/Automatic Operation Overview and System Design Guide

1.2.2 Language settings in the JP1/AO server OS

The table below describes the language (locale) settings supported by JP1/AO for each OS. Specify the settings correctly according to the table. If you specify language settings that are not shown here, text might be corrupted or defined information might be changed.

Table 1-2: OS language settings supported by JP1/AO

OS	Setting location	Value to be set			
		Japanese	English	Chinese	Other languages#
Windows	Control Panel	Japanese	English	Chinese (Simplified)	Regional and language options for the language
Linux	LANG environment variable	Set either of the following locales: • ja_JP.UTF-8 • ja_JP.utf8	Set C.	Set either of the following locales: • zh_CN.UTF-8 • zh_CN.utf8	Set any locale for the language.

#

Other languages here mean German, French, Spanish, Korean, and Russian. If one of these languages is set, text is displayed in English in windows. However, you can enter text using the other languages.

1.2.3 Check the port to use

Before you install JP1/AO on Linux 8, verify that the ports that JP1/AO will use on the JP1/AO server are not in use by other products. If a port is being used by another product, neither product might operate correctly.

To ensure that the necessary ports are not in use, use the `netstat` or `ss` command.

You must verify that port numbers 22170 - 22173 are not used by other products because this causes a new, overwrite, or upgrade installation to fail.

1.3 New installation of JP1/AO

1.3.1 Procedure to perform a new installation of JP1/AO

Use the Hitachi Integrated Installer or Hitachi Program Product Installer.

Before you begin

Perform all of the tasks that are required prior to installing JP1/AO, such as checking prerequisites.

To perform a new installation of JP1/AO:

1. Set the distribution media, and then execute the Hitachi Integrated Installer or Hitachi Program Product Installer.
   (If you choose to use the Hitachi Program Product Installer) For details about how to use the Hitachi Program Product Installer, see 1.3.2 Installation procedure using the Hitachi Program Product Installer. When installation by the Hitachi Program Product Installer finishes, perform the procedure from step 8.
2. Continue the configuration process as prompted by the wizard.#
   - Specify the JP1/AO installation folder.
3. Check the summary that is displayed to verify the settings that you have entered in the wizard thus far.#
   If necessary, you can click the **Edit settings** button and change the following items:
   - Installation folders for the databases
   - IP address or host name of the JP1/AO server
   - Port number of the JP1/AO server
   - Backup execution flag and backup folder
     As the preparation for an installation failure, specify whether to back up the databases that are shared with JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products and set the backup folder. You must set these items only when JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products have been already installed.
4. Click the **Install** button to start the installation of JP1/AO.
   When the installation of JP1/AO is complete, the JP1/AO - Contents installation wizard is displayed.#
5. Specify the JP1/AO - Contents installation folder.#
6. Check the summary that is displayed to verify the settings that you have entered in the wizard thus far.#
7. Click the **Install** button to start the installation of JP1/AO - Contents.#
8. If the OS is Windows, if you specify a port number that is not the default port number, you must perform the procedure for changing the port number.
9. After the installation is complete, execute the `hcmds64srv` command with the `start` option specified to start the JP1/AO services.
10. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO service templates provided by JP1/AO - Contents into JP1/AO.

#

If the Hitachi Program Product Installer is used, the installation wizard is not displayed during installation. When JP1/AO is installed, JP1/AO - Contents is also installed.

Important

- In Linux, do not specify a symbolic link as the installation destination. If you specify a symbolic link, installation will fail.
- If you interrupt the installation process, it might leave empty folders. You can manually delete any empty folders that were created.
- If Common Component fails to install and you have to reinstall, you cannot specify an installation destination that is different from the previous destination. Even if you enter a different destination, it will automatically be installed in the previous installation destination.

Results of procedure

- The product names listed below are displayed in the Programs and Features window displayed by clicking Windows **Control Panel**, **Programs** and then **Programs and Features**.

  Table 1-3: Product names displayed in the Programs and Features window

Product name	Version
JP1/Automatic Operation	*vv.rr.mm*
JP1/Automatic Operation - Contents	*vv.rr.mm*

- If the OS is Windows, **JP1_Automatic Operation** is added to **All Programs** in the Start menu.
- If the OS is Windows, some of the ports that JP1/AO uses for external connections are registered as firewall exceptions.

Related topics

- 1.3.3 Installation folder for each product
- 1.3.4 Installation folders for databases
- 1.3.5 Database backup folder
- JP1/AO services in the JP1/Automatic Operation Administration Guide
- List of shared built-in service properties in the JP1/Automatic Operation Administration Guide
- Ports used for JP1/AO external connections in the JP1/Automatic Operation Overview and System Design Guide

1.3.2 Installation procedure using the Hitachi Program Product Installer

The Hitachi Program Product Installer is contained on the JP1/AO distribution media. This subsection describes the following operations that you perform by using the Hitachi Program Product Installer:

- Starting the Hitachi Program Product Installer
- Using the Hitachi Program Product Installer to install JP1/AO
- Using the Hitachi Program Product Installer to uninstall JP1/AO
- Using the Hitachi Program Product Installer to check the versions of currently installed Hitachi products

For details about the procedures to be performed in the OS, see the documentation for the OS.

Pre-installation task

Log in to the JP1/AO server (server on which JP1/AO will be installed) with root permissions.

Starting the Hitachi Program Product Installer:

1. Set the JP1/AO distribution media.
2. Mount the distribution media. For details about how to mount the distribution media, see the documentation for the OS.

   `/bin/mount -r -o mode=0544 /dev/cdrom /mnt/cdrom`

   Note: The name of the device special file (*/dev/cdrom*) and the name of the mount-point directory for the file system of the distribution media (*/mnt/cdrom*) differ depending on the environment.
3. Start the Hitachi Program Product Installer.

   The directory and file names of the distribution media might be seen differently depending on the environment. Enter a file name in the same form as displayed by the `ls` command.

   `/mnt/cdrom/X64LIN/setup /mnt/cdrom`

   Note: For */mnt/cdrom*, specify the mount-point directory for the distribution media.
4. Unmount the distribution media.

   After installation is complete, unmount the distribution media. For details about how to unmount the distribution media, see the documentation for the OS.

   `/bin/umount /mnt/cdrom`

   Note: For */mnt/cdrom*, specify the mount-point directory for the distribution media.

Using the Hitachi Program Product Installer to install JP1/AO:

1. In the initial screen of the Hitachi Program Product Installer, enter `I`.

   A list of program products that can be installed is displayed.
2. Position the cursor at the product that you want to install, and then press the space bar to select that product.
3. Enter `I`.

   Installation of JP1/AO starts. After installation is complete, you can redisplay the initial screen by entering `Q`.

Execution result

Check the following installation log files:

- Under `/var/opt/jp1ao/logs`:
  JP1AO_Inst_*VV.R.R_yyyy-mm-dd-HH-MM-SS*.log[#1#2]
- Under `/var/opt/HiCommand/Base64/log/HInst`:
  inst_*yyyymmdd-HHMMSS-nn*.log[#3]
- Under `/tmp`:
  - hcmds64inst.log
  - hcmds64rtn.inst
  - hcmdshdb_result

#1

If installation is not completed, this log data might be stored under `/tmp`.

#2

VV.R.R indicates the version and revision numbers of JP1/AO. *yyyy-mm-dd* the execution date, and *HH-MM-SS* the execution time.

#3

yyyymmdd indicates the execution date, and *HHMMSS* indicates the execution time. *nn* is a two-digit generation number from 01 to 30.

Using the Hitachi Program Product Installer to uninstall JP1/AO:

1. Start the Hitachi Program Product Installer by executing the following command:
   `/etc/hitachi_setup`
2. In the initial screen that is displayed, enter `D`.
   A list of program products that can be uninstalled is displayed.
3. Position the cursor at the product that you want to uninstall, and then press the space bar to select the product.
4. Enter `D`.
   The selected program product is uninstalled. You can redisplay the initial screen by entering `Q`.

Execution result

Check the following uninstallation log files:

- Under `/tmp`:
  JP1AO_Uninstall.log
- Under `/var/opt/HiCommand/Base64/log/HInst`:
  uinst_yyyymmdd-HHMMSS-nn.log#

#

yyyymmdd indicates the execution date, and *HHMMSS* indicates the execution time. *nn* is a two-digit generation number from 01 to 30.

Using the Hitachi Program Product Installer to check the versions of currently installed Hitachi products:

1. Start the Hitachi Program Product Installer by executing the following command:
   `/etc/hitachi_setup`
2. In the initial screen that is displayed, enter `L`.
   A list of currently installed Hitachi program products is displayed.

1.3.3 Installation folder for each product

If the OS of the JP1/AO server is Windows, the installation folder of each product is specified by using the installation wizard. If the OS of the JP1/AO server is Linux, the installation folder is fixed and cannot be changed.

Table 1-4: Default installation folder (in Windows)

Item	Installation folder	Modifiable
JP1/AO	*system-drive*\Program Files\Hitachi\JP1AO#1	Y
JP1/AO - Contents	*system-drive*\Program Files (x86)\Hitachi\JP1AOCONT#2	Y
Common Component#3	*system-drive*\Program Files\Hitachi\HiCommand\Base64#4	Y

Legend:

Y: Can be modified.

#1

The `JP1AO` part is fixed. In this manual, JP1/AO installation folder refers to *system-drive*`\Program Files\Hitachi\JP1AO`.

#2

The `JP1AOCONT` part is fixed.

#3

This component is a collection of functions used in common with Hitachi Command Suite products. It is installed as one of the JP1/AO components.

If the Hitachi Command Suite products are installed, Common Component has already been installed in the folder that is created when the Hitachi Command Suite products are installed. In such a case, therefore, the *system-drive*\Program Files\Hitachi\HiCommand\Base64 folder is not created.

#4

The `HiCommand\Base64` part is fixed.

If you change the JP1/AO installation folder, it changes the *system-drive*`\Program Files\Hitachi` path.

#5

The `JP1Base` part is fixed.

Table 1-5: Installation folder (in Linux)

Item	Installation folder	Modifiable
JP1/AO	• /opt/jp1ao • /var/opt/jp1ao	N
JP1/AO - Contents	/opt/jp1aocont	N
Common Component#	/opt/HiCommand/Base64	N

Legend:

N: Cannot be modified.

#

This component consists of the functions that are shared by Hitachi Command Suite products. This component is installed as a function of the JP1/AO.

If one or more Hitachi Command Suite products have already been installed, Common Component has already been installed in a folder that was created when the first Hitachi Command Suite product was installed. In such a case, therefore, the `/opt/HiCommand/Base64` folder is not created.

If the OS of the JP1/AO server is Windows, do not specify any of the folders in the table below as the installation destination. Furthermore, do not specify the JP1/AO Content Pack installation folder (or its subfolder) as the installation destination of JP1/AO.

Table 1-6: Folders that cannot be specified as the installation destination

Folder	Remarks
Directly under the drive	You cannot specify a drive only, such as `c:\` or `d:\`.
32-bit application folder in 64-bit Windows	You cannot specify *%programfiles(x86)%*#, *%CommonProgramFiles(x86)%*#, *%WinDir%*, *%WinDir%\system32*, and *%programfiles%\WindowsApps*.

Folder	Remarks
Network drive	--

Legend:

--: None

#

The installation destination of JP1/AO - Contents can be specified.

Related topics

- 1.3.1 Procedure to perform a new installation of JP1/AO
- 1.3.6 Characters that can be specified in installation, database, and backup folder names
- 4.1 Procedure to change the JP1/AO installation folder

1.3.4 Installation folders for databases

If the OS of the JP1/AO server is Windows, the database installation folders can be specified. If the OS of the JP1/AO server is Linux, the database installation folders are fixed and cannot be changed.

Table 1-7: Default database installation folders (in Windows)

Item	Installation folder	Modifiable
JP1/AO database	*system-drive*\Program Files\Hitachi\HiCommand\database\Automation[#1]	Y
Common Component database	• *system-drive*\Program Files\Hitachi\HiCommand\database\BASE[#2] • *system-drive*\Program Files\Hitachi\HiCommand\database\SYS	Y

Legend:

Y: Can be modified.

#1

The `Automation` part is fixed.

#2

The `Base` part is fixed.

If you change the JP1/AO database installation folder, it changes the *system-drive*`\Program Files\Hitachi\HiCommand\database` path.

Table 1-8: Database installation folders (in Linux)

Item	Installation folder	Modifiable
JP1/AO database	/var/opt/HiCommand/database/x64/Automation	N
Common Component database	• /var/opt/HiCommand/database/x64/BASE • /var/opt/HiCommand/database/x64/SYS	N

Legend:

N: Cannot be modified.

Related topics

- 1.3.1 Procedure to perform a new installation of JP1/AO
- 1.3.6 Characters that can be specified in installation, database, and backup folder names
- 4.2 Procedure to change the database installation folder

1.3.5 Database backup folder

If the OS of the JP1/AO server is Windows, the dbexported_hdb folder is created as the database backup folder for the database specified in the installation wizard. If the OS of the JP1/AO server is Linux, the database backup folder is fixed and cannot be changed.

Table 1-9: Default backup folder

Item	Backup folder	Modifiable
Backup data of the database	For Windows: *system-drive*\Program Files\Hitachi\Automation_backup\dbexported_hdb#	Y
	For Linux: /var/opt/Automation_backup/dbexport_hdb	N

Legend:

Y: Can be modified.

N: Cannot be modified.

#

The `dbexported_hdb` part is fixed.

Related topics

- 1.3.1 Procedure to perform a new installation of JP1/AO
- 1.3.6 Characters that can be specified in installation, database, and backup folder names

1.3.6 Characters that can be specified in installation, database, and backup folder names

The following table lists the characters that can be used to specify the installation folder, database folder, and backup folder if the OS of the JP1/AO server is Windows.

Table 1-10: Characters that can be specified in the installation, database, and backup destination names

Item to be specified	Character string length	Characters that can be specified (single-byte characters)	Characters that cannot be specified
Installation folder	64 characters or less	A to Z, a to z, 0 to 9, _. ( ) space \ :	• Characters not listed in the *Characters that can be specified* column • Drive letters other than A to Z or a to z • A colon (:) used for other than a drive letter separator • Single-byte parentheses used for other than (x86) • . (current folder) • .. (parent folder) • A period at the end of the folder name • A backslash (\) used for other than a file separator • More than one consecutive backslash • More than one consecutive single-byte space • Single-byte spaces at the beginning of the path • OS reserved words (AUX, CON, NUL, PRN, CLOCK$, COM1 to COM9, LPT1 to LPT9)
Database installation folder	90 characters or less		
Backup folder	150 characters or less		

Related topics

- 1.3.3 Installation folder for each product
- 1.3.4 Installation folders for databases
- 1.3.5 Database backup folder

1.3.7 Characters that can be specified in the host name and IP address of the JP1/AO server

The table below lists the characters that can be specified in the host name and IP address of the JP1/AO server.

If the IP address is specified with a left square bracket ([) at the beginning and a right square bracket (]) at the end, it is treated as IPv6. In other cases, it is assumed that an IPv4 address or host name was entered.

Table 1-11: Characters that can be specified in the host name and IP address of the JP1/AO server

Item	Character string length	Characters that can be specified (single-byte characters)	Characters that cannot be specified
Host name or IPv4 address	32 bytes or less	Any	Any
IPv6 address	47 bytes or less (Including the opening [and closing])	A-F a-f 0-9 . : [ ]	• Characters not listed in the *Characters that can be specified* column • Four or more periods (.) • Eight or more colons (:) • [other than at the beginning of the line •] other than at the end of the line

1.4 Procedure to install the manual

If you install the manual on JP1/AO server, you will be able to access the manual by clicking the **Help** button in the main window of JP1/AO.

For a cluster system, follow the procedures to install the manual in both the active server and the standby server.

To install the manual:

1. Insert the manual distribution medium into the drive.
2. On the JP1/AO server, create folders with the names shown below. These are the folders into which the manuals will be copied.

Table 1-12: Installable manuals and the folders to be created (in Windows)

Manual	Folder to be created
IT Operations Automation: Getting Started	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOGS English environment: *JP1/AO-installation-folder*\docroot\help\en\AOGS Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOGS
JP1/Automatic Operation Overview and System Design Guide	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AODG English environment: *JP1/AO-installation-folder*\docroot\help\en\AODG Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AODG
JP1/Automatic Operation Configuration Guide	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOKG English environment: *JP1/AO-installation-folder*\docroot\help\en\AOKG Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOKG
JP1/Automatic Operation Administration Guide	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOUG English environment: *JP1/AO-installation-folder*\docroot\help\en\AOUG Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOUG
JP1/Automatic Operation Service Template Developer's Guide	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOSG English environment: *JP1/AO-installation-folder*\docroot\help\en\AOSG Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOSG
JP1/Automatic Operation Command and API Reference	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOGR

Manual	Folder to be created
JP1/Automatic Operation Command and API Reference	English environment: *JP1/AO-installation-folder*\docroot\help\en\AOGR Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOGR
JP1/Automatic Operation Service Template Reference	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOSR English environment: *JP1/AO-installation-folder*\docroot\help\en\AOSR Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOSR
JP1/Automatic Operation Messages	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOMR English environment: *JP1/AO-installation-folder*\docroot\help\en\AOMR Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOMR

Table 1-13: Installable manuals and the folders to be created (in Linux)

Manual	Folder to be created
IT Operations Automation: Getting Started	Japanese environment: /opt/jp1ao/docroot/help/ja/AOGS English environment: /opt/jp1ao/docroot/help/en/AOGS Chinese environment: /opt/jp1ao/docroot/help/zh/AOGS
JP1/Automatic Operation Overview and System Design Guide	Japanese environment: /opt/jp1ao/docroot/help/ja/AODG English environment: /opt/jp1ao/docroot/help/en/AODG Chinese environment: /opt/jp1ao/docroot/help/zh/AODG
JP1/Automatic Operation Configuration Guide	Japanese environment: /opt/jp1ao/docroot/help/ja/AOKG English environment: /opt/jp1ao/docroot/help/en/AOKG Chinese environment: /opt/jp1ao/docroot/help/zh/AOKG
JP1/Automatic Operation Administration Guide	Japanese environment: /opt/jp1ao/docroot/help/ja/AOUG English environment: /opt/jp1ao/docroot/help/en/AOUG Chinese environment: /opt/jp1ao/docroot/help/zh/AOUG
JP1/Automatic Operation Service Template Developer's Guide	Japanese environment: /opt/jp1ao/docroot/help/ja/AOSG

Manual	Folder to be created
JP1/Automatic Operation Service Template Developer's Guide	English environment: /opt/jp1ao/docroot/help/en/AOSG Chinese environment: /opt/jp1ao/docroot/help/zh/AOSG
JP1/Automatic Operation Command and API Reference	Japanese environment: /opt/jp1ao/docroot/help/ja/AOCR English environment: /opt/jp1ao/docroot/help/en/AOCR Chinese environment: /opt/jp1ao/docroot/help/zh/AOCR
JP1/Automatic Operation Service Template Reference	Japanese environment: /opt/jp1ao/docroot/help/ja/AOSR English environment: /opt/jp1ao/docroot/help/en/AOSR Chinese environment: /opt/jp1ao/docroot/help/zh/AOSR
JP1/Automatic Operation Messages	Japanese environment: /opt/jp1ao/docroot/help/ja/AOMR English environment: /opt/jp1ao/docroot/help/en/AOMR Chinese environment: /opt/jp1ao/docroot/help/zh/AOMR

3. For each manual, copy the files and folders listed below from the manual distribution medium.

Table 1-14: Files and folders to be copied and destination folders (for manuals)

Files and folders to be copied		Destination folders
If the OS of the JP1/AO server is Windows	If the OS of the JP1/AO server is Linux	
All HTML files, CSS files, and the GRAPHICS folder in *drive-on-which-manual-distribution-media-is-set*\MAN\3021*alphanumeric-based-on-manual-number*#	All HTML files, CSS files, and the GRAPHICS folder in */mount-point-for-manual-distribution-media*/MAN/3021/*alphanumeric-based-on-manual-number*#	Folders that you created in step 2

This alphanumeric omits the first four digits of the manual's document number and the hyphen (-) (such as 03D0100D).

For details about the relationship between manual names and document numbers, see *Reference material for this manual* in the *JP1/Automatic Operation Overview and System Design Guide*.

4. Delete the following file from the JP1/AO server:

Table 1-15: File to be deleted

The OS of the JP1/AO server	File to be deleted
Windows	• *JP1/AO-installation-folder*\docroot\help\ja\INDEX.HTM (for the Japanese environment) • *JP1/AO-installation-folder*\docroot\help\en\INDEX.HTM (for the English environment) • *JP1/AO-installation-folder*\docroot\help\zh\INDEX.HTM (for the Chinese environment)
Linux	• /opt/jp1ao/docroot/help/ja/INDEX.HTM (for the Japanese environment) • /opt/jp1ao/docroot/help/en/INDEX.HTM (for the English environment) • /opt/jp1ao/docroot/help/zh/INDEX.HTM (for the Chinese environment)

5. Copy the file shown below.

Table 1-16: File to be copied and destination folder (for INDEX.HTM)

Language settings in the JP1/AO server OS	File to be copied		Destination folder	
	If the OS of the JP1/AO server is Windows	If the OS of the JP1/AO server is Linux	If the OS of the JP1/AO server is Windows	If the OS of the JP1/AO server is Linux
Japanese environment	*JP1/AO-installation-folder* \docroot\help \INDEX_JA.HTM	/opt/jp1ao/docroot/help/INDEX_JA.HTM	*JP1/AO-installation-folder*\docroot\help\ja	/opt/jp1ao/docroot/help/ja
English environment	*JP1/AO-installation-folder* \docroot\help \INDEX_EN.HTM	/opt/jp1ao/docroot/help/INDEX_EN.HTM	*JP1/AO-installation-folder*\docroot\help\en	/opt/jp1ao/docroot/help/en
Chinese environment	*JP1/AO-installation-folder* \docroot\help \INDEX_EN.HTM	/opt/jp1ao/docroot/help/INDEX_EN.HTM	*JP1/AO-installation-folder*\docroot\help\zh	/opt/jp1ao/docroot/help/zh

6. Change the name of the copied file to INDEX.HTM.

Results of procedure

The manual is installed, and you can access the manual by clicking the **Help** button in the main window.

Related topics

- 1.1 New installation procedure
- 1.3.3 Installation folder for each product

1.5 Installing JP1/AO Content Pack

1.5.1 Procedure to install JP1/AO Content Pack

When you install JP1/AO Content Pack, you will be able to use service templates or Service Template Set in JP1/AO. To install JP1/AO Content Pack, use the Hitachi Integrated Installer or Hitachi Program Product Installer. The wizard will guide you through the procedure. For details about how to use the Hitachi Program Product Installer, see 1.3.2 Installation procedure using the Hitachi Program Product Installer. When installation by the Hitachi Program Product Installer finishes, perform step 4.

Before you begin

- Log in as a user with administrator or root permissions.
- Confirm that JP1/AO is installed.

  Note that because JP1/AO Content Pack does not conflict with other products, you do not have to check for conflicting products.

To install JP1/AO Content Pack:

1. Insert the distribution medium into the drive.
2. Specify the JP1/AO Content Pack installation folder, as prompted by the wizard.#

   Do not install JP1/AO Content Pack in the same installation folder as JP1/AO.
3. Click the **Install** button to start installation.#
4. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO service templates or Service Template Set into JP1/AO.

#

If the Hitachi Program Product Installer is used, the installation wizard is not displayed during installation.

Results of procedure

- The following product name is displayed in the Programs and Features window displayed by clicking Windows **Control Panel**, **Programs** and then **Programs and Features**.

  Product name:

  JP1/Automatic Operation Content Pack

  Version:

  vv.rr.mm
- Service Template Set is stored in the following folder:

  JP1/AO-Content-Pack-installation-folder\contents\setup or /opt/jp1aocont/contents/setup

  You can use the service template list displayed in the **Service Template** window to check whether service templates have been imported. You can also check this by executing the `listservices` command.

Related topics

- 1.5.2 JP1/AO Content Pack installation folder

1.5.2 JP1/AO Content Pack installation folder

If the OS of the JP1/AO server is Windows, the installation folder for JP1/AO Content Pack is specified by using the wizard during installation.

Do not specify the JP1/AO installation folder as the installation folder for JP1/AO Content Pack.

If the OS of the JP1/AO server is Linux, the installation folder for JP1/AO Content Pack is fixed and cannot be changed.

Table 1-17: Default installation folder for JP1/AO Content Pack

Item	Character string length	Installation folder	Modifiable
JP1/AO Content Pack	150 bytes or less	In Windows *system-drive*\Program Files (x86)\Hitachi\JP1AOCONTSET#	Y
		In Linux /opt/jp1aocontset	N

Legend:

Y: Can be modified.

N: Cannot be modified.

#

The `JP1AOCONTSET` part is fixed.

Related topics

- 1.5.1 Procedure to install JP1/AO Content Pack

1.6 Procedure to enable HTTPS connections between Web browsers and JP1/AO

1.6.1 Communication protocols available for JP1/AO for connecting to a Web browser

You can select HTTP or HTTPS connection for communication between Web browsers and JP1/AO. To use HTTPS connections, you need to acquire an SSL server certificate from the certificate authority (CA), and then specify the setting to enable HTTPS connections.

In JP1/AO, the HTTP connection is set by default.

For cluster systems, specify the settings to enable HTTPS connection on both the active server and the standby server.

1.6.2 Procedure to acquire an SSL server certificate necessary for HTTPS connections

Create a CSR file and send it to the CA to acquire an SSL server certificate.

Before you begin

- Log in to the JP1/AO server as a user with administrator or root permissions.

To acquire an SSL server certificate:

1. Execute the `hcmds64ssltool` command to save a private key file available for SHA256withRSA, and a CSR file that is to be sent to the CA.
2. Send the CSR file to the CA to acquire an SSL server certificate file (PEM format) available for SHA256withRSA.

1.6.3 Procedure to enable HTTPS connections (Windows, Linux 6, Linux 7, SUSE Linux 12)

Set up the user_httpsd.conf file, and then store the private key file and SSL server certificate file in the specified folder to enable HTTPS connections on the Web server.

Before you begin

- Log in to the JP1/AO server as a user with administrator or root permissions.
- Stop the JP1/AO service.

  For non-cluster systems:

  Execute the `hcmds64srv` command with the `stop` option specified.

  For cluster systems:

  Use the cluster software to bring the service offline.

To enable HTTPS connections:

1. Change the settings in the user_httpsd.conf file to enable HTTPS connection.

   The user_httpsd.conf file is stored in the following folder:

   - If the OS of the JP1/AO server is Windows
     Common-Component-installation-folder\uCPSB\httpsd\conf
   - If the OS of the JP1/AO server is Linux 6, Linux 7, SUSE Linux 12
     /opt/HiCommand/Base64/uCPSB/httpsd/conf

   Change the settings in the user_httpsd.conf file as follows:

   - Delete heading hash marks (#) from the Listen directive line on which the port number used for HTTPS connection is specified, and the following lines up to the HWSLogSSLVerbose On line, except the SSLECCCertificateKeyFile, SSLECCCertificateFile, SSLCACertificateFile, and Header set Strict-Transport-Security max-age=31536000 directive line.

     Note that you need to delete the hash mark (#) at the beginning of Listen [::]:22016 only if you want to enable communication with IPv6 addresses.
   - To disable all connections other than HTTPS connections, further change the settings as follows:

     • Add a hash mark (#) at the beginning of the Listen and Listen [::]: directive lines on which the port number used for HTTP connections is specified, to comment out the lines.

     • Delete the hash mark (#) at the beginning of the Listen 127.0.0.1: directive line.

   The following shows the initial settings (for HTTP connections) of the user_httpsd.conf file that exist when JP1/AO has just been installed, and the settings of that file changed to use HTTPS connections. In the following example, default port numbers are used: 22015 for HTTP connections and 22016 for HTTPS connections.

   Settings in the user_httpsd.conf file specified to use HTTP connections (initial settings):

```
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 TLSv12
#  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-GCM-SHA384:EC
DHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:AES256-G
CM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256
#  SSLRequireSSL
#  SSLCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf/s
sl/server/httpsdkey.pem"
#  SSLCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/
server/httpsd.pem"
#  SSLECCCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/con
f/ssl/server/ecc-httpsdkey.pem"
#  SSLECCCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/s
sl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ss
l/cacert/anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
#</VirtualHost>
#HWSLogSSLVerbose On
```

   Settings in the user_httpsd.conf file specified to use HTTPS connections (changed settings):

```
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 TLSv12
  SSLRequiredCiphers AES256-SHA256:AES256-SHA:AES128-SHA256:AES128-SHA:DES-CBC3-SH
A
  SSLRequireSSL
  SSLCertificateKeyFile "Common-Component-installation-folder/httpsd/conf/ssl/serv
er/httpsdkey.pem"
  SSLCertificateFile "Common-Component-installation-folder/httpsd/conf/ssl/server/
httpsd.pem"
# SSLECCCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf
/ssl/server/ecc-httpsdkey.pem"
# SSLECCCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ss
l/server/ecc-httpsd.pem"
# SSLCACertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl
/cacert/anycert.pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
HWSLogSSLVerbose On
```

Notes:

- For the ServerName directive in the top line and the ServerName directive in the <VirtualHost> tag, specify the host name (for cluster environments, specify the logical host name) that you specified for "Common Name" in the certificate signing request. Note that host names are case sensitive.
- For the SSLCertificateKeyFile directive, specify the absolute path of the private key file.

  Do not specify a symbolic link and junction for the path.
- For the SSLCertificateFile directive, specify the absolute path of the server certificate.

  There are two types of server certificates: certificates signed by a certificate authority and self-signed certificates.
- To use a certificate of the certificate authority, remove the hash mark (#) at the beginning of the line for the SSLCACertificateFile directive, and then specify the absolute path of the certificate of the certificate authority. Multiple certificates can be contained in one file by using a text editor to chain multiple PEM format certificates. Note that you must not specify a symbolic link or junction for the path.

2. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `start` option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

3. Update the URL information used for establishing a connection from the Web browser to the JP1/AO server.

   Execute the `hcmds64chgurl` command in the command prompt to update the URL information.

   For the URL, specify the host name or the IP address that is specified for the SSL server certificate.

4. If the OS of the JP1/AO server is Windows, change the URL of the shortcut file to the page displayed by performing the following operation:

   From the Start menu, select **All Program**, **JP1_Automatic Operation**, and then **JP1_AO Login**.

Important

If the connection between the Web browser and JP1/AO is configured incorrectly, the HBase 64 Storage Mgmt Web Service might fail to start, preventing the JP1/AO login window from appearing.

Related topics

- Login window in the JP1/Automatic Operation Administration Guide
- Maintenance in the JP1/Automatic Operation Administration Guide

1.6.4 Procedure to enable HTTPS connections (Linux 8)

Set up the user_httpsd.conf file, and then store the private key file and SSL server certificate file in the specified folder to enable HTTPS connections on the Web server.

Before you begin

- Log in to the JP1/AO server as a user with root permissions.
- Stop the JP1/AO service.

  For non-cluster systems:

  Execute the `hcmds64srv` command with the `stop` option specified.

  For cluster systems:

  Use the cluster software to bring the service offline.

To enable HTTPS connections:

1. Open the user_httpsd.conf file from the following location:
   Common-Component-installation-directory`/uCPSB11/httpsd/conf/user_httpsd.conf`
2. Within the user_httpsd.conf file, do the following:
   - Uncomment the following lines by removing the hash [#] signs:
     `#Listen 22016`
     through
     `#HWSLogSSLVerbose On`
     with the exception of `#SSLCACertificateFile` and `#Header set Strict-Transport-Security max-age=31536000`, which must remain commented out.
     For an IPv6 environment, remove the hash mark (#) at the beginning of the lines `#Listen [::]:22016`.
   - Edit the following lines as required:
     ServerName in the first line
     ServerName in the <VirtualHost> tag
     SSLCertificateKeyFile
     SSLCertificateFile
     #SSLCACertificateFile

When using a certificate of the certificate authority, delete the hash sign (#) from the line `#SSLCACertificateFile`, and specify the certificate of the certificate authority by using an absolute path.

Important

To block non-SSL communication from external servers to the host, 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`.

When editing directives, be aware of the following:

- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.
- When specifying paths in the following directives, do not specify symbolic links or junction points.
- When specifying certificates and private key files in the following directives, specify PEM-format files.
- Do not edit httpsd.conf and hsso_httpsd.conf files.

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
SSLEngine Off
#Listen [::]:22016
Listen 22016
<VirtualHost *:22016>
ServerName host-name
SSLEngine On
SSLProtocol +TLSv1.2
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE
-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-GCM-
SHA256
# SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECD
HE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256
SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/httpsdke
y.pem"
SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/httpsd.p
em"
# SSLCertificateKeyFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-http
sdkey.pem"
# SSLCertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/server/ecc-http
sd.pem"
SSLCACertificateFile
"Common-Component-installation-directory/uCPSB11/httpsd/conf/ssl/cacert/anycert.
pem"
# Header set Strict-Transport-Security max-age=31536000
</VirtualHost>
HWSLogSSLVerbose On
```

3. Start the JP1/AO service.
4. Update the JP1/AO URL by using the `hcmds64chgurl` command to do the following:

- Change the protocol from http: to https:
- Change the port number used for secure communication.

1.7 SSH connections with operation target devices

1.7.1 SSH connection authentication method available for JP1/AO

In JP1/AO, you can specify password authentication, public key authentication, or keyboard interactive authentication as an authentication method for SSH connections with operation target devices.

- Password authentication

  Password authentication is used for SSH connections with operation target devices. To set password authentication, you must specify the setting on the operation target devices to enable password authentication for the SSH server.
- Public key authentication

  A private key file is deployed in the JP1/AO server and public key files are deployed in operation target devices for SSH connections using public key authentication.
- Keyboard interactive authentication

  Keyboard interactive authentication is used for SSH connections with operation target devices. To set keyboard interactive authentication, you must specify the setting on the operation target devices to enable keyboard interactive authentication for the SSH server. Note that the keyboard interactive authentication available for JP1/AO supports only the `password` submethod.

Related topics

- 1.7.2 Public key authentication available for JP1/AO
- 1.7.4 Procedure to set public key authentication for SSH connections

1.7.2 Public key authentication available for JP1/AO

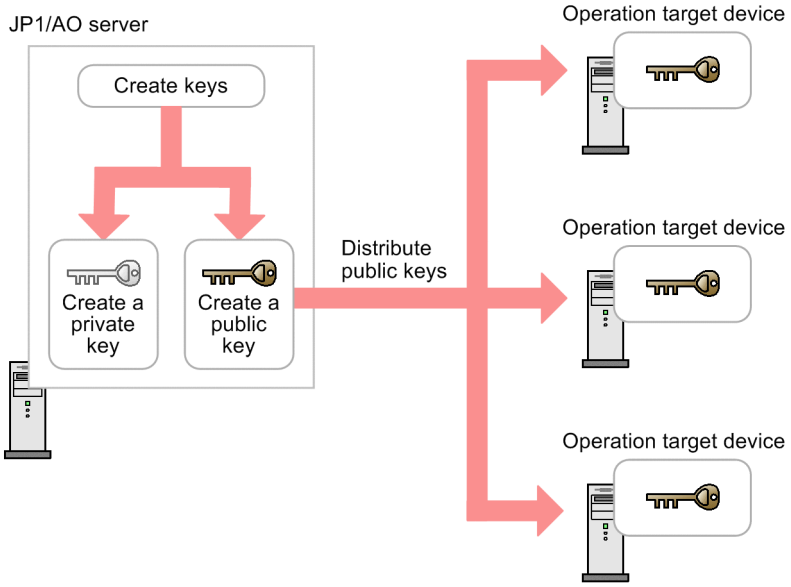
If you want to use public key authentication for SSH connections with operation target devices, you need to deploy a private key file on the JP1/AO server and a public key file on each operation target device.

Tip

The following shows an example in which a public key file and a private key file are created on the JP1/AO server. You can also create public key files and private key files on devices other than the JP1/AO server. In this case, the public key file corresponding to the private key file on the JP1/AO server must be deployed to each operation target device.

The following figure shows deployment of keys.

Figure 1-1: Deployment of keys for public key authentication



Related topics

- 1.7.4 Procedure to set public key authentication for SSH connections

1.7.3 Deploying public keys and private keys in a cluster configuration

If JP1/AO is used in a cluster configuration, how to deploy the public key files and private key files depends on whether the same key is used for the active and standby servers.

- To use the same key for the active server and the standby server:

  Copy the private key file from the active server to the standby server, and then deploy the public key file to operation target devices.

- To use different keys for the active server and the standby server:

  Create a public key and a private key on each active server and standby server, and then deploy both public key files to operation target devices.

In both cases, make sure that the private key file is deployed in the same path on both the active server and the standby server.

Tip

The following shows an example in which a public key file and a private key file are created on the JP1/AO server. You can also create public key files and private key files on devices other than the JP1/AO server. In this case, the public key file corresponding to the private key file on the JP1/AO server must be deployed to each operation target device.

The following figure shows deployment of keys in a cluster configuration.

Figure 1-2: Deployment of keys for public key authentication (using the same key for the active server and the standby server)

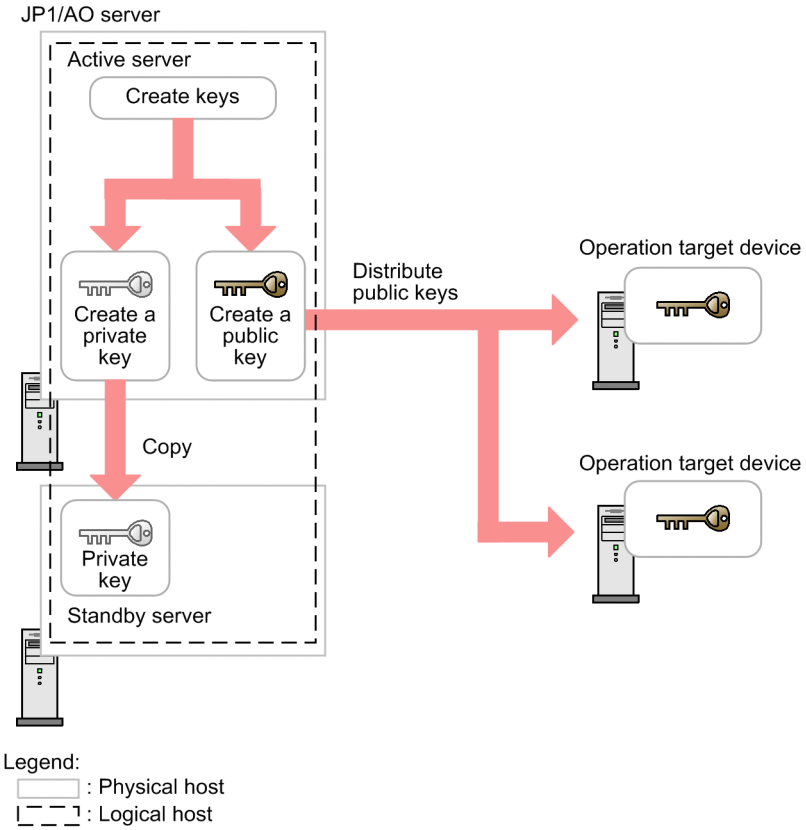
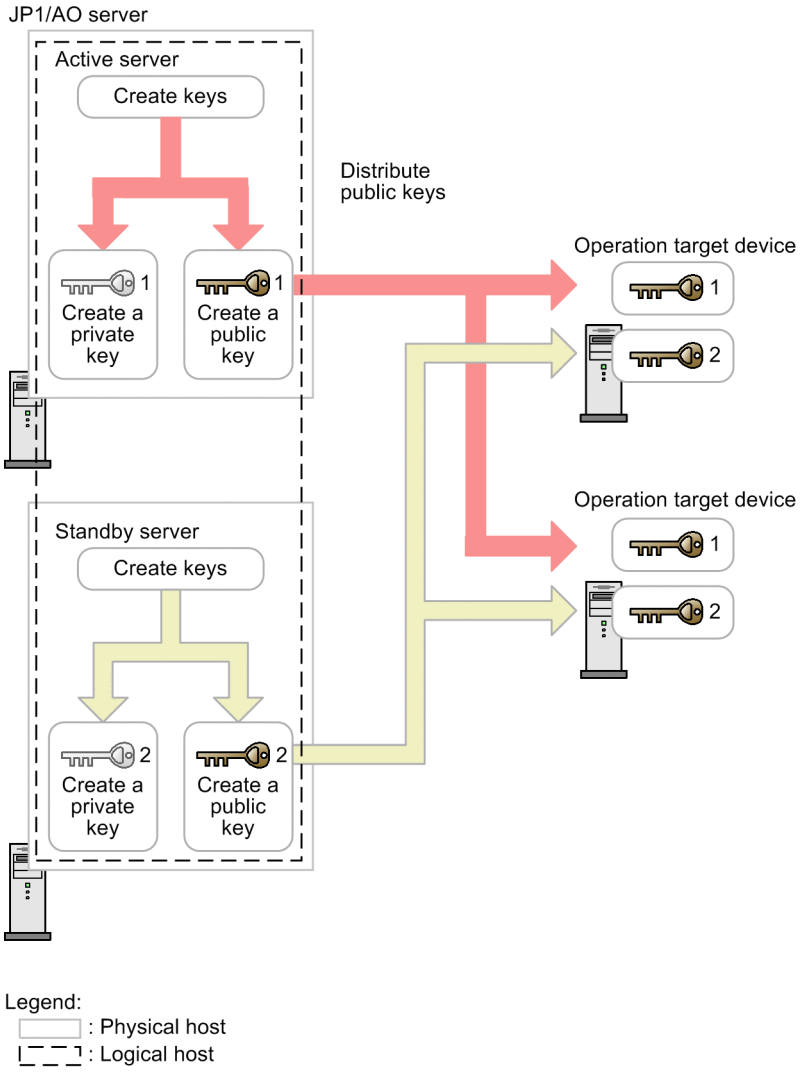


Figure 1-3: Deployment of keys for public key authentication (using different keys for the active server and the standby server)



1.7.4 Procedure to set public key authentication for SSH connections

Perform the following procedure to set public key authentication:

1. Set up the SSH server.
2. Create a public key file and a private key file.
3. Deploy the private key file to the JP1/AO server.
4. Specify a passphrase for the private key.
5. Deploy the public key file to operation target devices.

The following describes the details of each step.

For details about the procedure performed for an OS, see the OS documentation.

To set up the SSH server:

1. Log in to the target device as a root user.
2. Open the sshd_config file.
   The folder containing the file depends on the OS.
   - In HP-UX:
     /opt/ssh/etc/sshd_config
   - In OSs other than HP-UX:
     /etc/ssh/sshd_config
3. Set `yes` for the value of PubkeyAuthentication.
4. Execute the command to restart the sshd service. The following shows an example of executing the command for each OS.
   However, the command might be different depending on the OS version.
   - In Red Hat Enterprise Linux 8:
     `systemctl restart sshd`
   - In Red Hat Enterprise Linux 6.4:
     `/etc/rc.d/init.d/sshd restart`
   - In Solaris 10:
     `/usr/sbin/svcadm restart ssh`
   - In AIX 6.1:
     `kill -HUP` *`sshd-process-ID`*
   - In HP-UX 11i V3:
     `/sbin/init.d/secsh stop; /sbin/init.d/secsh start`

To create a public key and a private key:

Use the OS function or a tool to create a public key file and private key file. To use a tool, see the documentation of the tool for details about how to create the files.

Deploy the created private key file to the JP1/AO server, and the public key file to the operation target devices.

Tip

- We recommend that you create the public key file and private key file on the JP1/AO server. If you create these files on the JP1/AO server, there is no need to send the private key you created, thus allowing you to set public key authentication more safely.
- For the key type, you can select RSA encryption or DSA encryption.
- The permitted key length and key type depend on the OS. Create the public key file and private key file according to the OS specifications of the operation target device.
- Create a private key in PEM format.

The following shows an example of how to create the public key and private key for an operation target device.

1. Log in to the target device as a root user.
2. Execute the `ssh-keygen` command. Depending on the type of key to be created, enter as follows:

- To create an RSA key, enter:
  `ssh-keygen -t rsa`
- To create a DSA key, enter:
  `ssh-keygen -t dsa`

3. Specify the path and the file name used to output the private key.

   Do not include multibyte characters in the path and file name.

   A file containing the public key is output to the same path as the private key. The name of this file is the same as the private key file name with the extension `.pub`.

4. Specify a passphrase for the private key.

   When you are prompted to enter a passphrase for the private key, enter the passphrase, and then press the Return key. When you are prompted, enter the passphrase again, and then press the Return key.

   You can skip the specification of the passphrase. In this case, just press the Return key without entering anything.

5. Send the private key file you created to the JP1/AO server.

To deploy the private key to the JP1/AO server:

Use the following procedure to deploy the private key you created to the JP1/AO server:

1. Deploy the created private key file to any path on the JP1/AO server.
2. Specify the absolute path of the private key file for the ssh.privateKeyFile entry in the user-specified properties file (config_user.properties).
3. Stop the JP1/AO services.

   In a non-cluster system:

   Execute the `hcmds64srv` command with the `stop` option specified.

   In a cluster system:

   Use the cluster software to place the services offline.

4. Start the JP1/AO services.

   In a non-cluster system:

   Execute the `hcmds64srv` command with the `start` option specified.

   In a cluster system:

   Use the cluster software to place the services offline.

Tip

- We recommend that you deploy the private key file to a location other than in the JP1/AO installation folder. This is because if you deploy the private key file in the JP1/AO installation folder, the private key file is automatically deleted when JP1/AO is uninstalled.
- If JP1/AO is used in a cluster configuration, make sure that the private key file is deployed in the same path on both the active server and the standby server. You can use the same or different private keys for the active server and standby server.

To specify a passphrase for the private key:

Specify the passphrase for the JP1/AO shared built-in service property. Note that this step is not necessary if you specified a null character for the passphrase when creating the private key file.

1. In the **Administration** window, in the **Shared Properties Settings** area, select the **Pass phrase of the private key (for SSH public key authentication)** shared built-in service property, and then click the **Edit** button.
2. In the **Set Service Share Property** dialog box, select the **Change password** check box, and then, in the **Value** text box, enter the passphrase that was specified when the private key file was created.
3. Click the **OK** button.

To deploy the public key to an operation target device:

Use the following procedure to deploy the public key file to an operation target device.

1. Add the contents of the public key file to the authorized_keys file by, for example, redirecting the `cat` command.
2. Execute the `chmod` command to specify 700 for the attribute of the folder that contains the authorized_keys file. By default, this file is contained in the .ssh folder.
3. Execute the `chmod` command to specify 600 for the attribute of the authorized_keys file.

> **Tip**
>
> For JP1/AO used in a cluster configuration, if you want to use different private keys for the active and standby servers, deploy the public key file corresponding to the private key file on each server to operation target devices.

Related topics

- 1.7.3 Deploying public keys and private keys in a cluster configuration
- 2.2 User-specified properties file (config_user.properties)
- List of shared built-in service properties in the JP1/Automatic Operation Administration Guide

1.8 Procedure to import SSL server certificates for https connections between JP1/AO and external Web servers into Common Component

To enable https connections between JP1/AO and external Web servers, an SSL server certificate must be installed in the truststore of the Common Component. To import the SSL server certificate into the truststore of the Common Component, you use the `hcmds64keytool` command (in Windows) or the `keytool` command (in Linux).

Tip

You do not need to perform this procedure if you do not intend to use a Web client plug-in to establish https connections. You can also perform this procedure after you start using JP1/AO.

Before you begin

- Use a secure method to acquire the SSL server certificate to be imported.
- Check the path of the SSL server certificate to be imported.
- Check the path of the truststore file.

  In Windows:

  Common-Component-installation-folder`\uCPSB\jdk\jre\lib\security\jssecacerts`

  In Linux 6, Linux 7, SUSE Linux 12:

  Common-Component-installation-folder`/uCPSB/jdk/jre/lib/security/jssecacerts`

  In Linux 8:

  Common-Component-installation-folder`/uCPSB11/hjdk/jdk/lib/security/jssecacerts`
- Check the access password for the truststore.

Procedure to import SSL server certificate to truststore of Common Component

You can import an SSL server certificate into the truststore of the Common Component by executing a command. To import an SSL server certificate into the truststore of the Common Component:

1. Execute the following command:

   In Windows:

   Common-Component-installation-folder`\bin\hcmds64keytool -import -alias` *alias-name* `-file` *SSL-server-certificate-path* `-keystore` *truststore-file-path* `-storepass` *truststore-access-password*

   In Linux 6, Linux 7, SUSE Linux 12:

   Common-Component-installation-folder`/uCPSB/jdk/bin/keytool -import -alias` *alias-name* `-file` *SSL-server-certificate-path* `-keystore` *truststore-file-path* `-storepass` *truststore-access-password*

   In Linux 8:

   Common-Component-installation-folder`/uCPSB11/jdk/bin/keytool -import -alias` *alias-name* `-file` *SSL-server-certificate-path* `-keystore` *truststore-file-path* `-storepass` *truststore-access-password* `-storetype JKS`

Note

Note the following points when you specify *alias-name*, *truststore-file-path*, and *truststore-access-password* by using the `hcmds64keytool` or `keytool` command:

- For *alias-name*, specify the name used to identify the certificate within the truststore. If there are multiple SSL server certificates, specify an alias that is not already in use in the truststore.
- The following symbols cannot be used in *truststore-file-path*:
  Colons (:), commas (,), semicolons (;), asterisks (*), question marks (?), double quotation marks ("), left and right angle brackets (< and>), vertical bars (|), and hyphens (-)
- Specify *truststore-file-path* as a character string of 255 bytes or fewer.
- Double quotation marks (") cannot be used in *alias-name* or *truststore-access-password*.

2. Restart the JP1/AO server.

2 Post-Installation Environment Settings

This chapter describes the JP1/AO environment settings that are required during operation or before starting operation.

2.1 Procedure for setting the JP1/AO environment

The JP1/AO environment is set by editing definition files.

To set the JP1/AO environment:

1. Use a text editor to open the definition file for the relevant settings.

   Table 2-1: Settings and their definition files

Settings	Definition file to use	Reference
Various JP1/AO settings such as logs, tasks, and JP1 events	User-specified properties file (config_user.properties)	2.2 User-specified properties file (config_user.properties)
http port settings for executing commands	Command property file (command_user.properties)	2.3 Command property file (command_user.properties)
Settings for the title and body of email to be used in the notification by email function	Email notification definition files (mailDefinition_ja.conf, mailDefinition_en.conf, mailDefinition_zh.conf)	2.4 Email notification definition files (mailDefinition_ja.conf, mailDefinition_en.conf, mailDefinition_zh.conf)
Settings for user password conditions and locks	Security definition file (security.conf)	2.5 Security definition file (security.conf)
Settings for information used for connection with operation target devices	Connection-destination property file (*connection-destination-name*.properties)	2.6 Connection-destination property file (connection-destination-name.properties)
The character set specified for the JP1/AO server based on the character set information acquired from the operation target device	Character-set mapping file (charsetMapping_user.properties)	2.7 Character-set mapping file (charsetMapping_user.properties)
Settings for external authentication linkage	Configuration file for external authentication server linkage (exauth.properties)	2.8 Configuration file for external authentication server linkage (exauth.properties)
Settings for starting up JP1/AO when the OS starts (if the OS of the JP1/AO server is Linux)	OS startup script	2.9 Settings for automatically starting JP1/AO when the OS starts (in Linux)

2. Edit the definition files, and then save the changes.
3. Implement the contents of the definition files by restarting services or executing commands, as necessary.

Important

The line break code that can be used in definition files differs depending on the OS of the JP1/AO server. If the OS is Windows, CR+LF can be used. If the OS is Linux, LF can be used. For example, if you edit a definition file in a Windows environment, and then use the edited file in a Linux environment, use LF as the line break code.

2.2 User-specified properties file (config_user.properties)

This is the definition file used for various JP1/AO settings such as logs, tasks, and JP1 events.

Format

specification-key-name=setting

Installation folder

For non-cluster systems:

JP1/AO-installation-folder\conf or /opt/jp1ao/conf

For cluster systems:

shared-folder-name\jp1ao\conf or *shared-folder-name*/jp1ao/conf

Trigger for applying definitions

Restarting JP1/AO

Description

Specify one specification key name and its setting (value) in pairs per line. Note the following points when coding the user-specified properties file:

- Lines that begin with a hash mark (#) are treated as comments.
- Blank lines are ignored.
- The encoding is ISO 8859-1.
- The entries are case sensitive.
- To specify a backslash (\) in a character string, two backslashes (\\) must be entered.
  In this case, assume two backslashes as one byte to calculate the size.
- If an invalid value is entered for a setting, it is set to its default value, and the KNAE02022-W message 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

Table 2-2: Settings in the user-specified properties file

Classification	Key name	Settings	Specifiable values	Default value
Logs[#1]	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 (KB) for a server.	4-2,097,151	1,024
	logger.message.server.outputTaskDetail.enable	Specify whether to output detailed task information (KNAE01360-I, KNAE01361-W, or KNAE01362-E) to the server log. Nothing is output while debugging is being executed.	• true: Output • false: Do not output	false

Classification	Key name	Settings	Specifiable values	Default value
Logs[#1]	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 (KB) for a command.	4-2,097,151	1,024
	logger.TA.MaxFileSize	Specifies the maximum log file size (KB) for a task.	4-2,097,151	10,240
Task management	tasklist.autoarchive.taskRemainingPeriod	Specifies the period (days) that tasks whose execution has terminated are retained in the task list.	1-90	7
	tasklist.autoarchive.executeTime	Specifies the time at which the following processing is executed: • Automatic archive of tasks • Automatic deletion of history entries • Automatic deletion of debug tasks Invalid regions in the database are also released at this time.	00:00:00-23:59:59	04:00:00
	tasklist.autoarchive.maxTasks	Specifies the maximum sum of the number of tasks that can be kept in the task list and the number of debug tasks that can be kept in the debug task list.	100-5,000	5,000
	tasklist.autodelete.maxHistories	Specifies the maximum number of history entries that can be retained.	100-30,000	30,000
	task.periodicalTaskArchive.enable	Specify whether to periodically archive tasks and periodically delete task histories.	• true: Enable the function. • false:Disable the function.	false
	task.periodicalTaskArchive.period	Specify the execution intervals (unit: hour) for functions that periodically archive tasks and periodically delete task histories. Execution intervals are based on the execution time of the function that automatically archives tasks.	- 1 - 2 - 3 - 4 - 6 - 8 - 12 - 24	24
	task.periodicalTaskArchive.taskCountThreshold	Specify the threshold value of the number of tasks for periodically archiving tasks. Tasks are archived when the number of tasks exceeds the threshold value specified for this property. The value of this property must be less than the value of the tasklist.autoarchive.maxTasks key.	0-5000	4000
	task.periodicalTaskArchive.taskCountAfterArchive	Specify the number of remaining tasks for periodically archiving tasks. Tasks are periodically archived until the number of	0-5000	3000

Classification	Key name	Settings	Specifiable values	Default value
Task management	task.periodicalTaskArchive.taskCountAfterArchive	remaining tasks after archiving is the same as the value specified for this property. The value of this property must be less than the value of the task.periodicalTaskArchive.taskCountThreshold key.	0-5000	3000
	task.execute.skip.serverStart[#10]	Specifies the behavior of the task whose scheduled start time has passed when the JP1/AO service is restarted.	• true: The task enters Canceled status. • false: The task starts executing immediately.	false
Local execution of plug-ins	plugin.localMode	If you specify true, the execution user of the plug-in will be the System account or the root user. Note that the plug-in might not execute correctly if it uses resources that are unavailable to these users.	• true: Enable the function. • false:Disable the function.	false
Service management	packagemanager.maxServiceTemplates	Specifies the maximum number of service templates that can be managed in JP1/AO (total number of created and imported service templates).	1-3,000	1,000
	packagemanager.maxServices	Specifies the maximum number of services (including the debug service) that can be created.	1-3,000	1,000
JP1 event notifications	notification.jp1event	Specifies whether to send JP1 events in the notification function.	• true: Send • false: Do not send	false
Execution of plug-ins	plugin.threadPoolSize	Specifies the maximum number of plug-ins that can be executed concurrently.	• 10 • 50 • 100	10
Repeats	foreach.max_value	Specifies the maximum number of concurrent tasks that can be executed by a Repeated Execution Plug-in.	1-99	3
Remote connection port number	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
Terminal connection	plugin.terminal.prompt.account	Specifies a regular expression pattern (1-1,024 characters) used to detect the user ID waiting state. To establish a Telnet connection with the operation target device, if the standard output and standard error output match the specified regular expression, the terminal connect plug-in determines that a user ID must be entered. Then, this plug-in enters a user ID.	Character string that can be used in regular expression patterns	login|Login Name|Username|UserName

Classification	Key name	Settings	Specifiable values	Default value
Terminal connection	plugin.terminal.prompt.password	Specifies a regular expression pattern (1-1,024 characters) used to detect the password waiting state. To establish a Telnet connection with the operation target device, if the standard output and standard error output match the specified regular expression, the terminal connect plug-in determines that a password must be entered. Then this plug-in enters a password.	Character string that can be used in regular expression patterns	password|Password|PassWord
	telnet.connect.wait	Specifies the waiting time (seconds) until the standard output is returned after a Telnet connection is established with the operation target device.	1-600	60
	ssh.privateKeyFile	Specifies the absolute path of the private key file if public key authentication is used for SSH connections.	Character string of 0-255 characters	" " (null character)
Remote command	plugin.remoteCommand.executionDirectory.wmi[#2]	If the OS of the operation target device is Windows, this property specifies the path to the execution directory used to execute a content plug-in. Note that the execution directory must be created on the same drive as the work folder in advance. If necessary, the access permission settings of the execution directory must also be changed. At least the user who executes the plug-in must be given execute permission. If the execution mode of the content plug-in is Script, make sure that the total length (character count) of the value specified here and the script file name does not exceed 140 characters. If the total length exceeds 140 characters, forwarding of the script file might fail. We recommend that the value specified here is 50 or less characters because the script file name is specified using 90 or less characters.	Character string of 0-128 characters	" " (null character)
	plugin.remoteCommand.executionDirectory.ssh[#3]	If the OS of the operation target device is UNIX, this property specifies the path to the execution directory used to execute a content plug-in. Note that the execution directory must be created in advance. If necessary, the access permission settings of the execution directory must also be changed. At least the user who	Character string of 0-128 characters	" " (null character)

Classification	Key name	Settings	Specifiable values	Default value
Remote command	plugin.remoteCommand.executionDirectory.ssh[#3]	executes the plug-in must be given execute permission.	Character string of 0-128 characters	" " (null character)
	plugin.remoteCommand.workDirectory.ssh[#4]	If the OS of the operation target device is UNIX, this property specifies a work folder [#3] used to execute file-transfer plug-ins and content plug-ins. Enter a folder or symbolic link, using an absolute path of 1-128 characters. Symbolic links can be included in a layer of paths.[#5]	Single-byte alphanumeric characters, and the following symbols: / (used as a path separator), -, _, .	/tmp/Hitachi_AO
	plugin.wmi.win32.UACAdministratorsExec	Specify whether to enable the function for executing plug-ins by a user other than the System account when the OS of the destination host is Windows and UAC is enabled.	• true: Enable the function. • false:Disable the function.	false
	plugin.wmi.win32.CreationFlags.CREATE_NO_WINDOW	Enable this when the OS of the destination host is Windows and the command like that displays the progress bar may not work correctly if a user other than the System account executes the command.	• true: Enable the function. • false:Disable the function.	true
Web client	plugin.http.connect.timeout	Specifies the timeout value (seconds) for establishing an HTTP or HTTPS connection. If you specify 0, no timeout occurs.	0-3,600	60
	plugin.http.read.timeout	Specifies the timeout value (seconds) for reading data through an HTTP or HTTPS connection. If you specify 0, no timeout occurs.	0-86,400	600
remote host connection	plugin.adapter.timeout[#10]	Specifies the timeout value (seconds) for exclusive processing.	0-2147483647	2147483647
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 (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 Windows connection to the operation target device.	0-100	3
	wmi.connect.retry.interval	Specifies the interval (seconds) between retries, in the event of a failed Windows connection to the operation target device.	1-600	10
	telnet.connect.retry.times	Specifies the number of retries, in the event of a failed Telnet	0-100	3

Classification	Key name	Settings	Specifiable values	Default value
Retry remote host connection	telnet.connect.retry.times	connection to the operation target device.	0-100	3
	telnet.connect.retry.interval	Specifies the interval (seconds) between retries, in the event of a failed Telnet connection to the operation target device.	1-600	10
Retry remote file operation	plugin.remoteFileAccess.retry.times	Specifies the number of retries for a file manipulation command executed internally by a content plug-in or file-transfer plug-in. The retry interval is fixed at 100 ms. If a temporary file access error occurs, retrying the command might result in successful operation. However, if the file access error is not recovered, extra time is required for retries until the plug-in terminates. Specify this property in an environment in which file access errors occur even if there are no problems with disks.	0-100	0
Retry email sending	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 (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 the event of a failure of the Email Notification Plug-in to send an email.	0-100	3
	mail.plugin.retry.interval	Specifies the interval (seconds) between retries, in the event of a failure of the Email Notification Plug-in to send an email.	1-600	10
Audit log	logger.Audit.enable	Specifies whether to output the audit log.	• 0: Do not output • 1: Output	0
	logger.Audit.path	Specifies the output destination path of the audit log, using 1-244 bytes.	Single-byte alphanumeric characters, single-byte spaces, and the following symbols: !, #, $, &, (,), +, ,, -, ., ;, =, @, [,], ?, _, `, {, }, ~	In Windows: *JP1/AO-installation-folder*\logs[#6] In Linux: /var/opt/jp1ao/logs

Classification	Key name	Settings	Specifiable values	Default value
Audit log	logger.Audit.MaxBackupIndex	Specifies the maximum number of log backup files for the audit log.	1-16	7
	logger.Audit.MaxFileSize	Specifies the maximum log file size (KB) for the audit log.	4-2,097,151	1,024
	logger.Audit.command.useLoginUserID[#7]	Specifies whether to output the JP1/AO login user ID, in place of the user ID, to the subject identification information for the audit log when a command is executed.	• true: Output the JP1/AO login user ID to the subject identification information. • false: Output the OS user ID to the subject identification information.	false
Window refresh	client.events.refreshinterval	Specifies the refresh interval(seconds) for the Component area of the **Service Builder** window.	0-65,535	5
Service Builder	client.editor.upload.maxfilesize	Specifies the maximum file size (MB) that can be specified when one of the files is uploaded by using the **Service Builder** window: • Component icon file • Script file executed by a plug-in • Plug-in resource file • Service resource file • Window custom file	1-10	3
	server.editor.step.perTemplate.maxnum[#8]	Specifies the maximum number of steps per service template.	320-40,000 [#9]	320
	server.editor.step.perLayer.maxnum[#8]	Specifies the maximum number of steps per layer.	80-10,000 [#9]	80
	server.editor.publicProperty.perTemplate.maxnum	Specifies the maximum number of service properties per service template.	100-2,000	1,000
	server.editor.propertyGroup.perTemplate.maxnum	Specifies the maximum number of property groups per service template.	5-1,000	500
	client.editor.canvas.maxwidth[#8]	Specifies the maximum width (unit: px) of the operational region in the **Flow** area. The estimate expression is as follows: Width (px) = (number-of-steps-to-be-deployed-horizontally + 1) x 90 (px)	3,600-10,000	3,600
	client.editor.canvas.maxhigh[#8]	Specifies the maximum height (unit: px) of the operational region in the **Flow** area. The estimate expression is as follows: Height (px) = number-of-steps-to-be-deployed-vertically x 300 (px)	2,400-30,000	2,400

Classification	Key name	Settings	Specifiable values	Default value
Debug	tasklist.debugger.autodelete.taskRemainingPeriod	Specifies the period (days) that debug tasks whose execution has terminated are retained in the debug task list.	1-90	7
	client.debugger.tasklog.maxfilesize	Specifies the size of task logs (KB) displayed in the **Task Log** tab.	4-10,240	1,024
	logger.debugger.TA.MaxFileSize	Specifies the maximum log file size (KB) for a debug task.	4-2,097,151	10,240
Long-running tasks	server.longRunning.check.interval	Specifies the time (minutes) before the task is judged to be in Long Running status. If you specify 0, this judgment is not performed.	0-20,160	2,880
	server.longRunning.monitor.interval	Specifies the interval time (seconds) at which to monitor the tasks in Long Running status.	1-3,600	60
Output of plug-ins	plugin.stdoutSize.wmi	Specifies the maximum value (KB) of the total size of the standard output and standard error output if the connection target host is Windows in General Command Plug-in or the content plug-in. If the output exceeds the maximum value, execution of the plug-in becomes an error. If the number of line feeds in output becomes 65535 or more, since the plug-in remains running, specify a size that is within 65534.	1-1,024	100
	plugin.stdoutSize.ssh	Specifies the maximum value (KB) of the total size of the standard output and standard error output if the connection target host is UNIX, or if the connection protocol is SSH in Terminal Connect Plug-in or Terminal Command Plug-in. If the output exceeds the maximum value, execution of the plug-in be comes an error.	1-1,024	100
	plugin.stdoutSize.telnet	Specifies the maximum value (KB) of the total size of the standard output and standard error output if the connection protocol is Telnet in Terminal Connect Plug-in or Terminal Command Plug-in.	1-1,024	100
HTTP port number of Common Component	server.http.port	Specifies the HTTP port number of communication between JP1/AO server and Common Component	0-65535	22015

#1

The log output threshold for tasks can be set in the Service Share Properties.

#2

The execution directory name is determined from the following candidate values based on the indicated priority:

Priority	Candidate value
1	Execution directory value defined in the plug-in
2	Value specified for the common.executionDirectory key in the connection-destination property file (file name: connection destination name + .properties)
3	Value specified in plugin.remoteCommand.executionDirectory.wmi
4	Value of the Windows %TEMP% environment variable at the connection destination of the operation target device

#3

The execution directory name is determined from the following candidate values based on the indicated priority:

Priority	Candidate value
1	Execution directory value defined in the plug-in
2	Value specified for the common.executionDirectory key in the connection-destination property file (file name: connection destination name + .properties)
3	Value specified in plugin.remoteCommand.executionDirectory.ssh
4	/tmp

#4

Do not specify the path specified for this property or its parent folder's path for the source or destination folder for a file-transfer plug-in. If you specify such a folder, the property is not supported by the product.

#5

- The work folder must have read, write, and execution permissions for the connected user.
- When a file-transfer plug-in or content plug-in is executed, the access permission setting of the work folder is changed to 777, which permits all users to access the folder. If the path specified for the work folder does not exist when a file-transfer plug-in or content plug-in is executed, a work folder is created during execution of the plug-in. If an attempt to create the work folder fails, execution of the plug-in terminates abnormally.

#6

The name of an output file is Audit[n].log, where an integer indicating the number of files is displayed in [n].

#7

The user ID to be output to the subject identification information for the audit log can be changed when one of the following commands is executed:

- `deleteservicetemplate` command
- `importservicetemplate` command
- `listservices` command
- `listtasks` command
- `stoptask` command
- `submittask` command

#8

These properties are defined to provide compatibility with JP1/AO 10-02 or earlier.

#9

Edit these definitions only when all the conditions shown below exist. Note that the definitions must be edited before you duplicate or edit a service template.

- You are going to edit a service template created in JP1/AO 10-02 or earlier.
- The total number of steps in the service template to be edited exceeds 320, or the number of steps per layer exceeds 80.

#10

By default there is no key name in the file.

Example definitions

```
logger.message.server.MaxBackupIndex = 7
logger.message.server.MaxFileSize = 1024
logger.message.command.MaxBackupIndex = 7
logger.message.command.MaxFileSize = 1024
logger.TA.MaxFileSize = 10240
tasklist.autoarchive.taskRemainingPeriod = 7
tasklist.autoarchive.executeTime = 04:00:00
tasklist.autoarchive.maxTasks = 5000
tasklist.autodelete.maxHistories = 30000
task.periodicalTaskArchive.enable = false
task.periodicalTaskArchive.period = 24
task.periodicalTaskArchive.taskCountThreshold = 4000
task.periodicalTaskArchive.taskCountAfterArchive = 3000
plugin.localMode = false
packagemanager.maxServiceTemplates = 1000
packagemanager.maxServices = 1000
notification.jp1event = false
plugin.threadPoolSize = 10
foreach.max_value = 3
ssh.port.number = 22
telnet.port.number = 23
plugin.terminal.prompt.account = login|Login Name|Username|UserName
plugin.terminal.prompt.password = password|Password|PassWord
telnet.connect.wait = 60
ssh.privateKeyFile = C:\\ssh\\id_rsa
plugin.remoteCommand.executionDirectory.wmi = C:\\jp1ao
plugin.remoteCommand.executionDirectory.ssh = /home/jp1ao
plugin.remoteCommand.workDirectory.ssh = /tmp/Hitachi_AO
plugin.http.connect.timeout = 60
plugin.http.read.timeout = 600
ssh.connect.retry.times = 3
ssh.connect.retry.interval = 10
wmi.connect.retry.times = 3
wmi.connect.retry.interval = 10
telnet.connect.retry.times = 3
telnet.connect.retry.interval = 10
plugin.remoteFileAccess.retry.times = 0
mail.notify.retry.times = 3
mail.notify.retry.interval = 10
mail.plugin.retry.times = 3
mail.plugin.retry.interval = 10
logger.Audit.enable = 0
logger.Audit.path = C:\\Program Files\\Hitachi\\JP1AO\\logs
logger.Audit.MaxBackupIndex = 7
logger.Audit.MaxFileSize = 1024
logger.Audit.command.useLoginUserID = false
client.events.refreshinterval = 5
client.editor.upload.maxfilesize = 3
server.editor.step.perTemplate.maxnum = 320
```

```
server.editor.step.perLayer.maxnum = 80
server.editor.publicProperty.perTemplate.maxnum = 1000
server.editor.propertyGroup.perTemplate.maxnum = 500
client.editor.canvas.maxwidth = 3600
client.editor.canvas.maxhigh = 2400
tasklist.debugger.autodelete.taskRemainingPeriod = 7
client.debugger.tasklog.maxfilesize = 1024
logger.debugger.TA.MaxFileSize = 10240
server.longRunning.check.interval = 2880
server.longRunning.monitor.interval = 60
plugin.stdoutSize.wmi = 100
plugin.stdoutSize.ssh = 100
plugin.stdoutSize.telnet = 100
server.http.port = 22015
```

Related topics

- 2.1 Procedure for setting the JP1/AO environment

2.3 Command property file (command_user.properties)

This is the definition file for setting the http port that is used for executing commands.

If you change the port number used for communications between JP1/AO and the Web browser, you must also change the http port used for executing commands to the same number.

Format

specification-key-name=setting

Installation folder

For non-cluster systems:

JP1/AO-installation-folder\conf or /opt/jp1ao/conf

For cluster systems:

shared-folder-name\jp1ao\conf or *shared-folder-name*/jp1ao/conf

Trigger for applying definitions

Updating the definition file

Description

One specification key and setting can be specified per line. Note the following points when coding the command property file.

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- The encoding is ISO 8859-1.
- The entries are case sensitive.
- To specify a backslash (\) in a character string, two backslashes (\\) must be entered.
  In this case, assume two backslashes as one byte to calculate the size.
- If an invalid value is entered for a setting, it is set to its default value, and the KNAE02022-W message 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

Table 2-3: Settings in the command property file

Key name	Settings	Specifiable value	Default value
command.http.port	Specifies the http port used for executing commands.	1-65535	22015

Example definitions

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

Related topics

- 2.1 Procedure for setting the JP1/AO environment

2.4 Email notification definition files (mailDefinition_ja.conf, mailDefinition_en.conf, mailDefinition_zh.conf)

These are the definition files used for email notification in the event of a failure or if an abnormality is detected in a task.

Edit mailDefinition_ja.conf in a Japanese environment, mailDefinition_en.conf in an English environment, and mailDefinition_zh.conf in a Chinese environment.

Format

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

Installation folder

For non-cluster systems:

JP1/AO-installation-folder\conf or /opt/jp1ao/conf

For cluster systems:

shared-folder-name\jp1ao\conf or *shared-folder-name*/jp1ao/conf

Trigger for applying definitions

Restarting JP1/AO

Description

The email notification definition file is edited in XML format. The locations you can edit are *email-title* and *email-body*.

When editing the file, note the following points.

- A read error occurs if the email notification definition file 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 other than <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 tag entries are case sensitive.

Settings

Table 2-4: Settings in the email notification definition file

Settings	XML element	Character string length
Title of email to be used in email notifications	title	Character string of 0-9,999 bytes
Body of email to be used in email notifications	body	

Table 2-5: Default values of settings in the email notification definition file

Settings for:	Default title of email to be used in email notifications	Default body of email to be used in email notifications
Japanese environment	[Automatic Operation]$TASK_NAME$が $TASK_STATUS$に変更されました。	サービスグループ名:$SERVICE_GROUP_NAME$ タスク名:$TASK_NAME$ 実行者:$USER_NAME$ タスク詳細:$TASK_DETAIL_URL$
English environment	[Automatic Operation]$TASK_NAME$ has changed to $TASK_STATUS$	Service Group Name:$SERVICE_GROUP_NAME$ RESOURCE_GROUP_NAME$ Task Name:$TASK_NAME$ User Name:$USER_NAME$ Task Detail:$TASK_DETAIL_URL$
Chinese environment	[Automatic Operation]$TASK_NAME$已为$TASK_STATUS$状态。	服务组名:$SERVICE_GROUP_NAME$ 任务名:$TASK_NAME$ 执行者:$USER_NAME$ 任务详细内容:$TASK_DETAIL_URL$

If you want to use characters that are not valid in XML syntax in the title or body of the email, use XML entity references.

Table 2-6: XML entity references

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

The following embedded characters can be used in the title or body of the email.

Table 2-7: Embedded characters in the email notification definition file

Embedded characters	Item	Remarks
$SERVICE_GROUP_NAME$	Service group name	Set to the character string representing the service 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	
$TASK_TAGS$	Task tag	
$TASK_STATUS$	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	

Embedded characters	Item	Remarks
$SCHEDULE_PERIOD$	Scheduled execution period	Set according to the format in the task properties.
$SCHEDULE_TIME$	Scheduled execution time	
$SCHEDULE_ START_DATE$	Date execution was scheduled to start	
$USER_NAME$	User who executes the operation	
$TASK_DETAIL_URL$	URL of the **Task Details** window	Set to a URL starting with http or https.

Depending on the state of the relevant task, the values of some properties might be empty. In these cases, the embedded characters will be blank values.

Example definitions

Example notification that the status of a task has changed, giving the service group name, task name, user, and task details

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<mail xmlns="http://www.hitachi.com/products/it/software/xml/automation/conf/mailD
efinition">
<title>[Automatic Operation]$TASK_NAME$ has changed to $TASK_STATUS$</title>
<body>
Service Group Name:$SERVICE_GROUP_NAME$
Task Name:$TASK_NAME$
User Name:$USER_NAME$
Task Detail:$TASK_DETAIL_URL$
</body>
</mail>
```

Related topics

- 2.1 Procedure for setting the JP1/AO environment

2.5 Security definition file (security.conf)

This is the definition file for settings related to user password conditions and locks.

In a cluster system, make the settings the same on the active server and the standby server.

Format

specification-key-name=setting

Installation folder

Common-Component-installation-folder\conf\sec or /opt/HiCommand/Base64/conf/sec

Trigger for applying definitions

Updating the definition file

Description

One specification key and setting can be specified per line. Note the following points when coding the security definition file.

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- The entries are case sensitive.
- If an invalid value is specified, the default value will be set.
- If the same specification key is entered multiple times in a file, the last one that is specified will take effect.

Example definitions

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

Table 2-8: Settings in the security definition file

Key name	Settings	Specifiable value	Default value
password.min.length	Specifies the minimum number of characters in a password.	1-256	4
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 account is automatically locked. If 0 is specified, the account is not automatically locked after failed login attempts.	0-10	0

Related topics

- 2.1 Procedure for setting the JP1/AO environment

2.6 Connection-destination property file (connection-destination-name.properties)

This is the definition file for setting information used to establish connections when the following plug-ins are executed:

- General command plug-in
- File-transfer plug-in
- Terminal connect plug-in
- Content plug-in

Format

specification-key-name=setting

Installation folder

For non-cluster systems:

JP1/AO-installation-folder\conf\plugin\destinations or /opt/jp1ao/conf/plugin/destinations

For cluster systems:

shared-folder-name\jp1ao\conf\plugin\destinations or *shared-folder-name*/jp1ao/conf/plugin/destinations

Trigger for applying definitions

Executing a plug-in that references the connection-destination property file

Description

One specification key and setting can be specified per line. Note the following points when coding the connection-destination property file.

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- The encoding is ISO 8859-1.
- The entries are case sensitive.
- To specify a backslash (\) in a character string, two backslashes (\\) must be entered.
  In this case, assume two backslashes as one byte to calculate the size.
- If the same specification key is entered multiple times in a file, the last one that is specified will take effect.
- If an invalid value is specified in the connection-destination property file, an execution error occurs in the plug-in that references the connection-destination property file.
- The file name must be specified in the *host-name*`.properties` or *IP-address*`.properties` format. However, if you want to specify an IPv6 address, you must replace any colons (:) with a hyphen (-) because colons cannot be specified in a file name. For example, to specify the IPv6 address `2001::234:abcd`, enter `2001--234-abcd.properties`.

Settings

Table 2-9: Settings in the connection-destination property file

Key name	Settings	Specifiable values
terminal.charset	Specifies the character set used for communication.	• EUC-JP • eucjp • ibm-943C • ISO-8859-1 • MS932 • PCK • Shift_JIS • UTF-8 • windows-31j
telnet.port	Specifies the port number used for a Telnet connection by using the terminal connect plug-in. This setting has priority over the telnet.port.number setting in the user-specified properties file (config_user.properties).	0-65535
ssh.port	Specifies the port number used for an SSH connection by using one of the following plug-ins: • General command plug-in • File-transfer plug-in • Terminal connect plug-in • Content plug-in This setting has priority over the ssh.port.number setting in the user-specified properties file (config_user.properties).	0-65535
telnet.prompt.account	Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a user ID to establish a connection with the target device by using the terminal connect plug-in. You can use 1 to 1,024 characters. For example, specify `Username:`.	Character string that can be used in regular expression patterns
telnet.prompt.password	Specifies a regular expression pattern used to detect the character string that is output for prompting the user to enter a password to establish a connection with the target device by using the terminal connect plug-in. You can use 1 to 1,024 characters. For example, specify `Password:`.	Character string that can be used in regular expression patterns
telnet.noStdout.port.list	Specifies the port number of the service that does not return the standard output after a connection is established by using the terminal connect plug-in. You can use 1 to 1,024 characters. To specify multiple port numbers, use a comma as a separator.	0-65535, and commas (,)
wmi.workDirectory.sharedPath	Specifies the absolute path of the shared folder that stores the file to be transferred during command execution when a general command plug-in, file-transfer plug-in, or content plug-in is executed. The absolute path that you specify can have a maximum of 80 characters. The *value-of-this-property*\Hitachi\CMALib\JP1AO folder is created, and then, in that folder, the `home` and `launcher` folders are created. You must specify this property in the following cases:	Single-byte alphanumeric characters, backslashes (\), colons (:), hyphens (-), underscores (_), and periods (.)

Key name	Settings	Specifiable values
wmi.workDirectory.sharedPath	• The OS of the operation target device is Windows Server in a cluster configuration. • The logical host name or logical IP address is used to connect to the operation target device. If you specify this property, you must also specify the wmi.workDirectory.sharedName property. In addition, you must specify the same folder name for this property and the wmi.workDirectory.sharedName property. If you do not specify this property, the following folder is created. • When JP1/AO is in a non-cluster configuration or is on the active server of a cluster configuration: *%windir%*\Hitachi\CMALib\JP1AO • When JP1/AO is on the standby server of a cluster configuration: *%windir%*\Hitachi\CMALib\JP1AO_2	Single-byte alphanumeric characters, backslashes (\), colons (:), hyphens (-), underscores (_), and periods (.)
wmi.workDirectory.sharedName	Specifies the name (share name) of the shared folder that stores the file to be transferred during command execution when a general command plug-in, file-transfer plug-in, or content plug-in is executed. The shared folder name that you specify can have a maximum of 80 characters. The *value-of-this-property*\Hitachi\CMALib\JP1AO folder is created, and then, in that folder, the `home` and `launcher` folders are created. You must specify this property in the following cases: • The OS of the operation target device is Windows Server in a cluster configuration. • The logical host name or logical IP address is used to connect to the operation target device. This property must be specified when the wmi.workDirectory.sharedPath property is specified, as in the following example: wmi.workDirectory.sharedPath = F:\\work wmi.workDirectory.sharedName = work	Single-byte alphanumeric characters, hyphens (-), underscores (_), and periods (.)
wmi.adapter.id	In a Windows environment, specify this when you want to execute general command plug-ins, file-transfer plug-ins, and custom plug-ins to a Windows connection destination from multiple JP1/AO servers. For this property, specify a different value for each JP1/AO in the system. The maximum number of JP1/AO servers that connect to a Windows connection destination at the same time is 2. In a Windows environment, specify this when, with respect to a device that is being operated that exists on both a physical host and a logical host of the same host, you want to execute general command plug-ins, file-transfer plug-ins, and custom plug-ins at the same time. For this property, in the connection-destination property file of each logical host, specify a different value for each logical host. You can specify either 1 or 2 characters for the value of this property. You cannot specify "2" (1 character) for the value of this property. The value specified for this property is used as part of the name of the shared folder that stores files transferred at the time of command execution. When specifying this property, you must specify both wmi.workDirectory.sharedPath and	Single-byte alphanumeric characters

Key name	Settings	Specifiable values
wmi.adapter.id	wmi.workDirectory.sharedName. The "*property-specified-for-wmi.workDirectory.sharedPath*\Hitachi\CMALib\JP1AO_*value-specified-for-this-property*" folder is created, and the "home" and "launcher" folders are created inside the folder. If the local execution function is enabled and the operation target device is the local host, the specification of this property is invalid.	Single-byte alphanumeric characters
wmi.win32.UACAdministratorsExec	Specify whether to enable the function for executing plug-ins by a user other than the System account when the OS of the destination host is Windows and UAC is enabled. This setting has priority over the plugin.wmi.win32.UACAdministratorsExec setting in the user-specified properties file (config_user.properties).	• true: Enable the function. • false:Disable the function.
wmi.win32.CreationFlags.CREATE_NO_WINDOW	Enable this when the OS of the destination host is Windows and the command like that displays the progress bar may not work correctly if a user other than the System account executes the command. This setting has priority over the plugin.wmi.win32.CreationFlags.CREATE_NO_WINDOW setting in the user-specified properties file (config_user.properties).	• true: Enable the function. • false:Disable the function.
ssh.workDirectory	Specifies the absolute path of the work folder that is used when a file-transfer plug-in or content plug-in is executed for an operation target device whose OS is UNIX. #1 The absolute path you specify can have a maximum of 128 characters. You can specify a folder or symbolic link. You can also include a symbolic link in the path. If the specified value is invalid, the file-transfer plug-in or content plug-in terminates abnormally. This product does not support a case where a file-transfer plug-in is executed for the folder whose path is specified in this property or for the parent folder of that folder. The permission setting of the work folder must grant read, write, and execute permissions to the connected user. If the path specified in this property does not exist when a file-transfer plug-in or content plug-in is executed, a folder is created when the plug-in is executed. If the folder cannot be created, the plug-in terminates abnormally. The permission setting of the work folder must be changed to 777 regardless of whether the work folder already exists or is newly created.	Single-byte alphanumeric characters, forward slashes (/), hyphens (-), underscores (_), and periods (.)
common.executionDirectory	If the OS of the operation target device is Windows#2 This property specifies the path of the execution directory that is used to execute a content plug-in. Note that the execution directory must be created in advance on the same drive as the work folder. If necessary, the permission settings of that directory must also be changed. At least the user who executes the plug-in must be given execute permission.	Character string having a maximum of 128 characters

Key name	Settings	Specifiable values
common.executionDirectory	If Execution Mode of a content plug-in is Script, the total length of the value specified here and script file name must not exceed 140 characters. If the total length exceeds 140 characters, transfer of the script file might fail. Note that the maximum length of the script file is 90 characters. Therefore, we recommend that you use a maximum of 50 characters to specify the value of this property. If the OS of the operation target device is Linux[#3] This property specifies the path of the execution directory that is used to execute a content plug-in. Note that the execution directory must be created in advance. If necessary, the permission settings of that directory must also be changed. At least the user who executes the plug-in must be given execute permission.	Character string having a maximum of 128 characters

#1

The work directory is decided based on the following priority.

Priority	Setting value
1	Value specified for ssh.workDirectory
2	Value specified for plugin.remoteCommand.workDirectory.ssh in the user-specified properties file (config_user.properties)
3	/tmp/Hitachi_AO

#2

The execution directory name is determined from the following candidate values based on the indicated priority:

Priority	Candidate value
1	Execution directory value defined in the plug-in
2	Value specified for the common.executionDirectory key
3	Value specified for the plugin.remoteCommand.executionDirectory.wmi key in the user-specified properties file (config_user.properties)
4	Value of the Windows %TEMP% environment variable at the connection destination of the operation target device

#3

The execution directory name is determined from the following candidate values based on the indicated priority:

Priority	Candidate value
1	Execution directory value defined in the plug-in
2	Value specified for the common.executionDirectory key
3	Value specified for the plugin.remoteCommand.executionDirectory.ssh key in the user-specified properties file (config_user.properties)
4	/tmp

Example definition

```
terminal.charset=UTF-8
telnet.port=23
```

```
ssh.port=22
telnet.prompt.account=login
telnet.prompt.password=password
telnet.noStdout.port.list=25,80,110
```

2.7 Character-set mapping file (charsetMapping_user.properties)

This is the definition file for setting the character set for the JP1/AO server based on the character set information acquired from the operation target device.

Format

specification-key-name=setting

Installation folder

For non-cluster systems:

JP1/AO-installation-folder\conf\plugin or /opt/jp1ao/conf/plugin

For cluster systems:

shared-folder-name\jp1ao\conf\plugin or *shared-folder-name*/jp1ao/conf/plugin

Trigger for applying definitions

Restarting JP1/AO

Description

One specification key and setting can be specified per line. For the specification key name, the value of the `/usr/bin/locale charmap` command returned from the operation target device must be specified as is. If the returned value contains a double-quotation mark ("), add the double-quotation mark to the specified value. For *setting*, specify the character set that corresponds to the specification key name.

You can specify the following character sets:

- EUC-JP
- eucjp
- ibm-943C
- ISO-8859-1
- MS932
- PCK
- Shift_JIS
- UTF-8
- windows-31j

Note the following points when coding the character-set mapping file.

- Lines that begin with # are treated as comments.
- Blank lines are ignored.
- The encoding is ISO 8859-1.
- The entries are case sensitive.
- To specify a backslash (\) in a character string, two backslashes (\\) must be entered.
  In this case, assume two backslashes as one byte to calculate the size.

- If the same specification key is entered multiple times in a file, the last one that is specified will take effect.
- If an invalid value is specified in the character-set mapping file, an execution error occurs in the plug-in that references the character-set mapping file.

Example definitions

If the operation target device is HP-UX:

```
"utf8.cm" = UTF-8
"iso88591.cm" = ISO-8859-1
"SJIS.cm" = Shift_JIS
"eucJP.cm" = EUC-JP
```

2.8 Configuration file for external authentication server linkage (exauth.properties)

This is the definition file used to specify the settings required for external authentication linkage.

Format

specification-key-name=setting

Installation folder

Common-Component-installation-folder\conf or /opt/HiCommand/Base64/conf

Trigger for applying definitions

Immediately after the configuration file is saved

However, for any user who had already logged in when definitions of the configuration file were changed, the changes are not applied until the user logs in again. The authentication method displayed for such users might be different from the one used for login.

Description

One specification key and setting can be specified per line. Note the following points when coding the configuration file for external authentication server linkage:

- Lines that begin with # are treated as comment lines.
- Blank lines are ignored.
- The entries are case sensitive.
- Spaces cannot be specified before or after a setting.
- Do not enclose a setting in double quotation marks (").

Settings

Table 2-10: Settings in the configuration file for external authentication server linkage

Classification	Key name	Settings	Specifiable values	Default values
Common item	auth.server.type	Specifies the type of external authentication linkage.	• internal: Do not use external authentication linkage. • jp1base: Use external authentication linkage with JP1/Base. • ldap: Use external authentication linkage with Active Directory used as an LDAP directory server.	internal

Classification	Key name	Settings	Specifiable values	Default values
Common item	auth.server.name	Specifies the server identifier of the external authentication server to be linked. You can use a maximum of 64 bytes. You must specify this property if `ldap` is specified for `auth.server.type`. For other cases, there is no need to specify this property.	• ASCII printable character code (0x21-7E) excluding the following special characters: , \, /, :, ,, ;, *, ?, ", <, >, |, $, %, &, ', `	-- (Initial value at installation: ServerName)
	auth.group.mapping	Specifies whether to link groups if external authentication linkage with Active Directory is used.	• true: Link groups. • false: Do not link groups.	false
LDAP settings[#1]	auth.ldap.*server-identifier*[#2].protocol	Specifies the protocol for connecting to the LDAP directory server. There is no need to specify this property if a value other than `ldap` is specified for `auth.server.type`. If "`tls`" is specified, the encryption method used by the LDAP directory server differs depending on the JP1/AO version. Must be one of the following: • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA	• ldap: Performs communication by using plain text • tls: Performs communication by using StartTLS	--
	auth.ldap.*server-identifier*[#2].host	Specifies the host name, IPv4 address, or IPv6 address of the LDAP directory server. To specify an IPv6 address, enclose the value in square brackets ([ ]). You must specify this property if auth.ldap.*server-identifier*.dns_lookup is set to false. If "`tls`" is specified for "`auth.ldap.`*server-identifier*`.protocol`", it is necessary to specify the same host name as the CN of the server certificate of the LDAP directory server. An IP address cannot be used.	Character string that can be specified for host names or IP addresses	--
	auth.ldap.*server-identifier*[#2].port	Specifies the port number of the LDAP directory server.	1-65535	389
	auth.ldap.*server-identifier*[#2].timeout	Specifies the connection timeout period (seconds) with the LDAP directory server. Specify 0 to wait for a connection until a communication error occurs.	0-120	15

Classification	Key name	Settings	Specifiable values	Default values
LDAP settings[#1]	auth.ldap.*server-identifier*[#2].attr	Specifies the attribute name for which the user ID of the authentication user is defined.	Character string that can be used for attribute names	-- (Initial value at installation: sAMAccountName)
	auth.ldap.*server-identifier*[#2].basedn	Specifies the distinguished name (DN) used as the base point to search for the authentication user of the LDAP directory server.	Character string that can be used for DNs	--
	auth.ldap.*server-identifier*[#2].retry.interval	Specifies the interval (seconds) between retries in the event of a failed connection to the LDAP directory server.	1-60	1
	auth.ldap.*server-identifier*[#2].retry.times	Specifies the number of retries, in the event of a failed connection to the LDAP directory server.	0-50	20
	auth.ldap.*server-identifier*[#2].domain.name	Specifies the domain name of the LDAP directory server. You must specify this property if either of the following conditions is satisfied: • auth.group.mapping is set to true. • auth.ldap.*server-identifier*.dns_lookup is set to true, and auth.ldap.*server-identifier*.host is omitted.	Character string that can be specified for domain names	--
	auth.ldap.*server-identifier*[#2].dns_lookup	Specifies whether to use DNS to search for the LDAP directory server.	• true: Use DNS • false: Do not use DNS	false

#1

The settings are ignored if a value other than `ldap` is specified for `auth.server.type`.

#2

For *server-identifier*, specify the same value specified for *server-identifier* for `auth.server.name`.

Example definitions

- Example definition if all the following conditions exist:
  - External authentication linkage with Active Directory is used.
  - You do not want to link groups.
  - There is no need to register LDAP search users.
  - DNS is not used.

```
auth.server.type=ldap
auth.server.name=ServerName1
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.host=adhost1
auth.ldap.ServerName1.attr=cn
auth.ldap.ServerName1.basedn=cn=Users,dc=example,dc=com
```

- Example definition if all the following conditions exist:
  - External authentication linkage with Active Directory is used.
  - You want to link groups.

- LDAP search users need to be registered.
- DNS is used.

```
auth.server.type=ldap
auth.server.name=ServerName1
auth.ldap.ServerName1.protocol=ldap
auth.ldap.ServerName1.attr= sAMAccountName
auth.ldap.ServerName1.basedn=dc=example,dc=com
auth.ldap.ServerName1.domain.name=example.com
auth.ldap.ServerName1.dns_lookup=true
auth.group.mapping=true
```

Related topics

- 3.2 Linking with Active Directory

2.9 Settings for automatically starting JP1/AO when the OS starts (in Linux)

If the OS of the JP1/AO server is Linux, with the initial settings, the JP1/AO service is not automatically started when the OS starts.

For the JP1/AO service to start automatically when the OS starts, perform one of the following methods.

For Linux 8, use the method in CASE1. Also, replace `uCPSB` that is included in the path specified in the script file with `uCPSB11`.

CASE1: Set a new environment to use `systemd` (such as Red Hat Enterprise Linux 7)

- Setting method

  1. Create a Unit file of the automatic startup script for the JP1/AO service.
     Storage location: `/usr/lib/systemd/system`

     File name: `JP1_AO.service`

     If the file name is different, replace the part of "`JP1_AO.service`" in the following description.

     The number on the left are line number. Line without line number are continued from the line above.

```
 1 [Unit]
 2 Description=JP1/AO service
 3 After=2248-PD01.service hicommand64-hcs_hweb.service hicommand64-hcs_hsso.ser
   vice hicommand64-hcs_web.service hicommand64-hcs_ao.service
 4 Requires=2248-PD01.service hicommand64-hcs_hweb.service hicommand64-hcs_hsso.
   service hicommand64-hcs_web.service hicommand64-hcs_ao.service
 5
 6 [Service]
 7 Type=forking
 8 Environment="LANG=ja_JP.utf8"
 9 ExecStartPre=/home/jp1ao/ao_start_check
10 ExecStart=/opt/HiCommand/Base64/bin/hcmds64srv -start -server AutomationWebSe
   rvice
11 TimeoutStartSec= 600
12
13 [Install]
14 WantedBy=multi-user.target graphical.target
```

  2. Execute the following command to set up the attributes.

```
chmod 644 /usr/lib/systemd/system/JP1_AO.service
chgrp root /usr/lib/systemd/system/JP1_AO.service
chown root /usr/lib/systemd/system/JP1_AO.service
```

  3. Create a script file specified in the `ExecStartPre` option.

     `/home/jp1ao/ao_start_check`

```
#!/bin/sh
HCMDS_HOME=/opt/HiCommand/Base64

for i in `seq 1 10`
do
    cjstartsv_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/CC/server/bin/cjstartsv | grep -v grep | wc -l`
    hcs_hsso_counter=`ps -ef | \
    grep \
    ${HCMDS_HOME}/uCPSB/CC/server/repository/HBase64StgMgmtSSOService/hcs_hsso |
    \
```

```
    grep -v grep | wc -l`
    httpsd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/httpsd/sbin/httpsd | grep -v grep | wc -l`
    rotatelogs_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/httpsd/sbin/rotatelogs | grep -v grep | wc -l`
    pdprcd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdprcd | grep -v grep | wc -l`
    pdmlgd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdmlgd | grep -v grep | wc -l`
    pdrdmd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdrdmd | grep -v grep | wc -l`
    sleep 60

    if [ $cjstartsv_counter -ge 1 -a \
         $hcs_hsso_counter -ge 1 -a \
         $httpsd_counter -ge 22 -a \
         $rotatelogs_counter -ge 4 -a \
         $pdprcd_counter -ge 1 -a \
         $pdmlgd_counter -ge 1 -a \
         $pdrdmd_counter -ge 1 ]; then
         exit 0
    fi
done

exit 1
```

4. Execute the following command to set the attributes.
   ```
   chmod 554 /home/jp1ao/ao_start_check
   chgrp root /home/jp1ao/ao_start_check
   chown root /home/jp1ao/ao_start_check
   ```
5. Execute the following command to enable automatic startup of the JP1/AO service.
   ```
   systemctl daemon-reload
   systemctl enable JP1_AO.service
   ```
6. Execute the following command and confirm that "`enabled`" is displayed.
   ```
   systemctl list-unit-files | grep "UNIT FILE\|JP1_AO.service"
   ```

- Release method

1. If JP1/AO is running, execute the following command to stop JP1/AO.
   ```
   /opt/HiCommand/Base64/bin/hcmds64srv -stop
   ```
2. Execute the following command to disable automatic startup for the JP1/AO service.
   ```
   systemctl disable JP1_AO.service
   ```
3. Execute the following command and check that "`disabled`" is displayed.
   ```
   systemctl list-unit-files | grep "UNIT FILE\|JP1_AO.service"
   ```
4. Execute the following command to delete the Unit file for the JP1/AO service.
   ```
   rm -i /usr/lib/systemd/system/JP1_AO.service
   ```
5. Execute the following command to delete the script file.
   ```
   rm -i /home/jp1ao/ao_start_check
   ```

CASE2: Already configured in an environment that uses `systemd` (such as Red Hat Enterprise Linux 7)

If automatic startup has already been set up in the existing environment using the following method and there is no problem, there is no need to change the setting.

If automatic startup fails using the following method, cancel the following settings and then perform the setting method for CASE1.

- Setting method
  1. Create a Unit file of the automatic startup script for the JP1/AO service.
     Storage location: `/etc/systemd/system`
     File name: `JP1_AO.service`
     If the file name is different, replace the part of "`JP1_AO.service`" in the following description.

```
[Unit]
Description=JP1/AO service

[Service]
Type=forking
Environment="LANG=ja_JP.utf8"
ExecStart=/opt/HiCommand/Base64/bin/hcmds64srv -start -server AutomationWebServi
ce

[Install]
WantedBy=multi-user.target graphical.target
```

  2. Execute the following command to set up the attributes.
     `chmod 644 /etc/systemd/system/JP1_AO.service`
     `chgrp root /etc/systemd/system/JP1_AO.service`
     `chown root /etc/systemd/system/JP1_AO.service`
  3. Execute the following command to enable automatic startup for the JP1/AO service.
     `systemctl daemon-reload`
     `systemctl enable JP1_AO.service`
  4. Execute the following command and check that "`enabled`" is displayed.
     `systemctl list-unit-files | grep "UNIT FILE\|JP1_AO.service"`
- Release method
  1. If JP1/AO is running, execute the following command to stop JP1/AO.
     `/opt/HiCommand/Base64/bin/hcmds64srv -stop`
  2. Execute the following command to disable automatic startup for the JP1/AO service.
     `systemctl disable JP1_AO.service`
  3. Execute the following command and check that "`disabled`" is displayed.
     `systemctl list-unit-files | grep "UNIT FILE\|JP1_AO.service"`
  4. Execute the following command to delete the Unit file for the JP1/AO service.
     `rm -i /etc/systemd/system/JP1_AO.service`

CASE3: Environments that use automatic startup scripts (such as Red Hat Enterprise Linux 6)

- Setting method
  In the startup script of the OS, specify the value that is set in the LANG environment variable and specify a setting that executes the `hcmds64srv` command.
  Because the services of the common component are set to start automatically at OS startup, you must specify "`AutomationWebService`" as the `server` option so that only the JP1/AO service will be started.

When only the JP1/AO service is started with the `server` option specified, it is necessary to start the common component and database services beforehand. Therefore, it is necessary to check to see whether the JP1/AO service is started after checking the existence of common component and database process.

When the OS is stopped, the JP1/AO service and the services of the common component are set to automatically stop, so you do not need to set automatic stop.

Example:

```
#!/bin/sh
# chkconfig: 2345 99 01
# description: JP1/Automatic Operation
PROG_NAME=startao

start() {
    /home/jp1ao/startao2 &
}

case "$1" in
  start)
    start
    ;;
  *)
    echo "Usage: ${PROG_NAME} start"
    exit 1
esac
exit 0
```

/home/jp1ao/startao2

```
#!/bin/sh
HCMDS_HOME=/opt/HiCommand/Base64

start() {
    export LANG=ja_JP.utf8
    ${HCMDS_HOME}/bin/hcmds64srv -start -server AutomationWebService
    rtn_code=$?
    logger -i -s -t [AUTOMATION] \
   "${HCMDS_HOME}/bin/hcmds64srv -start -server AutomationWebService[${rtn_code}]"
}

for i in `seq 1 10`
do
    cjstartsv_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/CC/server/bin/cjstartsv | grep -v grep | wc -l`
    hcs_hsso_counter=`ps -ef | \
    grep \
    ${HCMDS_HOME}/uCPSB/CC/server/repository/HBase64StgMgmtSSOService/hcs_hsso | \
    grep -v grep | wc -l`
    httpsd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/httpsd/sbin/httpsd | grep -v grep | wc -l`
    rotatelogs_counter=`ps -ef | \
    grep ${HCMDS_HOME}/uCPSB/httpsd/sbin/rotatelogs | grep -v grep | wc -l`
    pdprcd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdprcd | grep -v grep | wc -l`
    pdmlgd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdmlgd | grep -v grep | wc -l`
    pdrdmd_counter=`ps -ef | \
    grep ${HCMDS_HOME}/HDB/lib/servers/pdrdmd | grep -v grep | wc -l`
    sleep 60

    if [ $cjstartsv_counter -ge 1 -a \
         $hcs_hsso_counter -ge 1 -a \
         $httpsd_counter -ge 22 -a \
         $rotatelogs_counter -ge 4 -a \
```

```
          $pdprcd_counter -ge 1 -a \
          $pdmlgd_counter -ge 1 -a \
          $pdrdmd_counter -ge 1 ]; then
        start
        exit 0
    fi
done

logger -i -s -t [AUTOMATION] "Common Component seems to be dead."
exit 1
```

- Release method

  1. If JP1/AO is running, execute the following command to stop JP1/AO.
     ```
     /opt/HiCommand/Base64/bin/hcmds64srv -stop
     ```
  2. Delete the created startup script.
  3. Execute the following command to delete the script file.
     ```
     rm -i /home/jp1ao/startao2
     ```

3 Linking to other products

This chapter describes linking between JP1/AO and other products.

3.1 Linking to the JP1/Base authentication function

3.1.1 Procedure for linking to the JP1/Base authentication function

This procedure requires setting up the configuration file for external authentication server linkage and creating and configuring JP1 users.

To link to the JP1/Base authentication function, perform the procedure described below.

Table 3-1: Procedure to link to the JP1/Base authentication function

Task		Required/ optional	Reference
1	If this is the first time you have linked JP1/AO to the JP1/Base authentication function, set up the configuration file for external authentication server linkage.	Required	3.1.2 Procedure for setting up the configuration file for external authentication server linkage
2	Create and configure JP1 users. This task can be performed safely before task 1.	Required	3.1.3 Procedure to create and configure JP1 users (JP1/Base linkage)
3	To confirm that the JP1 users created in task 2 can connect to JP1/Base, execute the `hcmds64checkauth` command.	Required	3.1.5 Procedure to check the link to JP1/Base

Related topics

- Linking with JP1/Base authentication in the JP1/Automatic Operation Administration Guide

3.1.2 Procedure for setting up the configuration file for external authentication server linkage

Set up the configuration file for external authentication server linkage in order to access the JP1/Base authentication function.

To use the JP1/Base authentication function, you also need to create and configure JP1 users. Before or after the steps below, create and configure the JP1 users that will be managed by the JP1/Base authentication function.

In a cluster system, make the settings the same on both the active server and the standby server.

To link to the JP1/Base authentication function:

1. Open the configuration file for external authentication server linkage (exauth.properties).
   This file is stored in the following folder:
   Common-Component-installation-folder\conf or /opt/HiCommand/Base64/conf
2. Specify the value `jp1base` for the specification key `auth.server.type`.
3. Save the changes to the configuration file for external authentication server linkage.

Related topics

- 3.1.3 Procedure to create and configure JP1 users (JP1/Base linkage)
- 2.8 Configuration file for external authentication server linkage (exauth.properties)

3.1.3 Procedure to create and configure JP1 users (JP1/Base linkage)

In order to manage JP1/AO user accounts by using the JP1/Base authentication function, you first create and configure the JP1 users.

In a cluster system, make the settings the same on both the active server and the standby server.

To create and configure JP1 users:

1. Create users in the JP1/Base operations window.
   To link JP1/AO to JP1/Base, you do not need to register users or user groups in the JP1/AO operations window.
2. In JP1/Base, specify a JP1 resource group name and permission level.
   For the JP1 resource group name, specify a JP1/AO service group name. Note, however, that if the name you specify is invalid as a JP1 resource group name, user authentication cannot be performed with JP1/Base.
   To grant All Service Groups permission, specify an asterisk (*) as the JP1 resource group name.

Related topics

- User Management Setup in the JP1/Base User's Guide
- 3.1.4 Defining permission levels in JP1/Base (JP1/Base linkage)

3.1.4 Defining permission levels in JP1/Base (JP1/Base linkage)

In order to link to JP1/Base, you must define JP1/Base permission levels based on the user's roles in JP1/AO.

Permission levels JP1_AO_Admin and JP1_AO_Develop can only be set to the JP1 resource group name `*`. If you set JP1_AO_Admin or JP1_AO_Develop to a JP1 resource group name other than `*`, that user will not be able to log in to JP1/AO.

In a cluster system, make the settings the same on both the active server and the standby server.

Table 3-2: Defining permission levels (JP1/Base link)

Role or authority in JP1/AO	JP1/AO permission level to be specified in JP1/Base
Admin	JP1_AO_Admin
Develop	JP1_AO_Develop
Modify	JP1_AO_Modify
Submit	JP1_AO_Submit
UserManagement	HCS_UserMng_Admin

Note that if the jp1admin user created by default during JP1/Base installation logs in to JP1/AO, it is treated as a user who has been granted UserManagement permissions and Admin role for `All Service Groups`.

If you use JP1/Base earlier than version 10-10, change the JP1/Base access permission level file as shown below, and then execute the `jbsaclreload` command.

Table 3-3: Definitions of the access permission level file

File path	File name	Item to be changed	Definition to be changed
For Windows: *system-drive*\Program Files (x86)\Hitachi\JP1Base\conf\user_acl# For Linux: /etc/opt/jp1base/conf/user_acl	JP1_AccessLevel	; for JP1/Automatic Operation	JP1_AO_Admin:AO:Admin,Develop,Modify,Execute,View JP1_AO_Develop:AO:Develop,Modify,Execute,View JP1_AO_Modify:AO:Modify,Execute,View JP1_AO_Submit:AO:Execute,View HCS_UserMng_Admin:HBase:Admin

#

system-drive\Program Files (x86)\Hitachi\JP1Base\ is the default installation location of JP1/Base. If the user has changed the installation location, a path different from this path is displayed.

Related topics

- User Management Setup in the JP1/Base User's Guide
- Evaluating users and access permissions in the JP1/Automatic Operation Overview and System Design Guide
- jbsaclreload in the JP1/Base User's Guide

3.1.5 Procedure to check the link to JP1/Base

After you create and configure JP1 users, check whether each user is able to connect to JP1/Base.

For a cluster system, follow the same steps on the active server and the standby server.

To check the link to JP1/Base:

1. Execute the `hcmds64checkauth` command.

Related topics

- hcmds64checkauth in the manual JP1/Automatic Operation Command and API Reference

3.2.1 Procedure to link with Active Directory

To link with Active Directory, you can select whether to link groups.

If you do not link groups, register the same user in both JP1/AO and Active Directory, and then use Active Directory to perform user authentication. There is no need to register a password in JP1/AO.

If you link groups, Active Directory groups registered as JP1/AO user groups are used. Therefore, create Active Directory groups to be registered as JP1/AO user groups as needed, and then add users who want to log in to JP1/AO to the Active Directory groups.

The table below describes the procedure to link with Active Directory. In a cluster system, make the settings the same on both the active server and the standby server.

Table 3-4: Procedure to link with Active Directory

Task		Do not link groups	Link groups	Reference
1	Register users in Active Directory.	Optional#1	Optional#1	3.2.2 Registering users in Active Directory
2	In the configuration file for external authentication server linkage, register information necessary for Active Directory linkage.	Required	Required	3.2.3 Registering information in the configuration file for external authentication server linkage
3	Evaluate the DIT structure of Active Directory, and then register LDAP search users or information in the configuration file for external authentication server linkage.	Required	Required	3.2.4 Registering LDAP search information
4	Set security for communication with the LDAP directory server.	Optional#2	Optional#2	3.2.8 Security settings for communication with the LDAP directory server
5	Execute the `hcmds64checkauth` command to confirm that JP1/AO can be linked with Active Directory by using the information registered in the configuration file for external authentication server linkage.	Required	Required	3.2.5 Checking JP1/AO connection with Active Directory
6	Register users in JP1/AO. It is not a problem to perform this task before task 1.	Required	Not required	3.2.6 Registering user information in JP1/AO
7	Assign roles to Active Directory groups.	Not required	Required	3.2.7 Assigning roles to Active Directory groups

#1

This task is not required if users that are registered in Active Directory log in to JP1/AO.

#2

This task is not required if "ldap" was specified as the protocol for connecting to the LDAP directory server.

Tip

A distinguished name (DN) registered in settings in the configuration file for external authentication server linkage cannot contain surrogate pair characters.

To link groups, the relative distinguished name (RDN) at the beginning of the DN of an Active Directory group must satisfy the conditions of the character code and character string length permitted for JP1/AO user groups.

Related topics

- Linking with Active Directory in the JP1/Automatic Operation Administration Guide

3.2.2 Registering users in Active Directory

In Active Directory, register users who want to log in to JP1/AO. This task is not required if users registered in Active Directory log in to JP1/AO.

If you link groups, use Active Directory groups registered as JP1/AO user groups. Therefore, if necessary, create Active Directory groups that are to be registered as JP1/AO user groups, and then add users who want to log in to JP1/AO to the Active Directory groups.

If you do not link groups, make sure that Active Directory user IDs match the JP1/AO user IDs.

3.2.3 Registering information in the configuration file for external authentication server linkage

In the configuration file for external authentication server linkage (exauth.properties), register information necessary for Active Directory linkage.

The configuration file for external authentication server linkage is stored in the following folder:

Common-Component-installation-folder\conf or /opt/HiCommand/Base64/conf

Table 3-5: Information that can be registered in the configuration file for external authentication server linkage

Key name	Settings	Definition
auth.server.type	ldap (fixed)	Required
auth.server.name	Server identifier	Required
auth.group.mapping	true: Link groups. false: Do not link groups.	Required
auth.ldap.*server-identifier*.protocol	ldap: Performs communication by using plain text tls: Performs communication by using StartTLS	Required
auth.ldap.*server-identifier*.host	Host name or IP address of the LDAP directory server	Optional[#1]
auth.ldap.*server-identifier*.port	Port number of the LDAP directory server	Optional
auth.ldap.*server-identifier*.timeout	Connection timeout period (seconds) for the LDAP directory server	Optional
auth.ldap.*server-identifier*.retry.interval	Interval (seconds) between retries, in the event of a failed connection to the LDAP directory server	Optional

Key name	Settings	Definition
auth.ldap.*server-identifier*.retry.times	Number of retries, in the event of a failed connection to the LDAP directory server	Optional
auth.ldap.*server-identifier*.domain.name	Domain name	Optional[#2]
auth.ldap.*server-identifier*.dns_lookup	true: Use DNS to search for the LDAP directory server. false: Do not use DNS to search for theLDAP directory server.	Optional

#1

You must specify this property if auth.ldap.*server-identifier*.dns_lookup is set to false.

If "tls" is specified for "auth.ldap.*server-identifier*.protocol", it is necessary to specify the same host name as the CN of the server certificate of the LDAP directory server. An IP address cannot be used.

#2

You must specify this property if either of the following conditions exists:

- auth.group.mapping is set to true.
- auth.ldap.*server-identifier*.dns_lookup is set to true, and auth.ldap.*server-identifier*.host is omitted.

Related topics

- 2.8 Configuration file for external authentication server linkage (exauth.properties)

3.2.4 Registering LDAP search information

Active Directory linkage uses simple authentication that requires DNs. In addition, LDAP search information is required to search for user information in Active Directory.

LDAP search information includes:

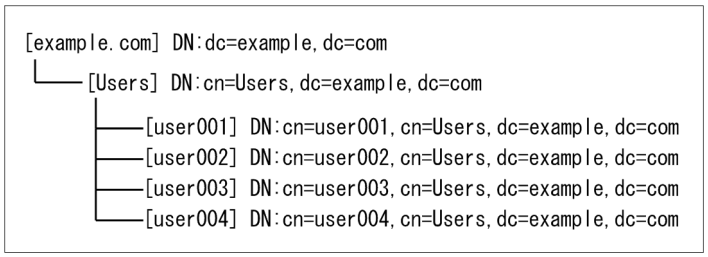
- Information specified in the configuration file for external authentication server linkage
- LDAP search users

LDAP search information to be registered depends on whether information entries for users who log in to JP1/AO are listed under a DN in the DIT (Directory Information Tree) structure. Therefore, you must first check the DIT structure, and then register LDAP search information. In addition, if you specify to link groups, you need to register LDAP search users, regardless of the DIT structure.

1. Check the DIT structure and determine the required tasks.
   - In the DIT structure, if user entries of all users who want JP1/AO link with Active Directory are listed directly under a particular DN, there is no need to register LDAP search users.

     The following shows an example of the DIT structure for which there is no need to register LDAP search users.

Figure 3-1: Example of DIT structure (if there is no need to register LDAP search users)



In this example, there is no need to register LDAP search users because all user entries are listed directly under one DN (`cn=Users,dc=example,dc=com`). If there is no need to register LDAP search users, go to step 2.

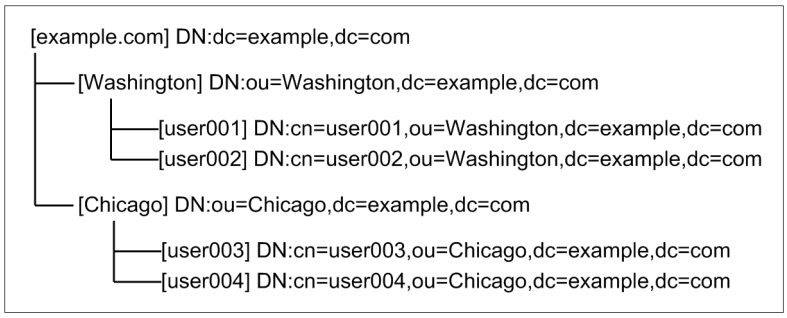
However, there is an exception even if the condition shown in this example is satisfied. Specifically, if the attribute value of the RDN does not match the JP1/AO user ID in the user entry of the same user, you need to register LDAP search users. In this case, go to step 3.

- In the DIT structure, if user entries of users who want JP1/AO link with Active Directory are listed under multiple DNs in Active Directory, you do not need to register LDAP search users.

  In a Windows environment, you cannot use Japanese for search user DNs.

  The following shows an example of the DIT structure for which you need to register LDAP search users.

Figure 3-2: Example of DIT structure (if you need to register LDAP search users)



In this example, you need to register LDAP search users because user entries are listed under two DNs (`ou=Washington,dc=example,dc=com` and `ou=New York,dc=example,dc=com`).

If you need to register LDAP search users, go to step 3.

2. Perform the task applicable if there is no need to register LDAP search users.

   Register information in the configuration file for external authentication server linkage according to the following table.

Table 3-6: Setting in the configuration file for external authentication server linkage (if there is no need to register LDAP search users)

Key name	Settings
auth.ldap.*server-identifier*#.attr	Attribute name of the user entry RDN
auth.ldap.*server-identifier*#.basedn	DN one layer above the user entry

#: Register the settings defined for the `auth.server.name` key.

3. Perform the task applicable if you need to register LDAP search users.

   - Execute the `hcmds64ldapuser` command to register LDAP search users.
   - Register information in the configuration file for external authentication server linkage according to the following table.

Table 3-7: Setting in the configuration file for external authentication server linkage (if you need to register LDAP search users)

Key name	Settings
auth.ldap.*server-identifier*#.attr	Attribute name with a user ID
auth.ldap.*server-identifier*#.basedn	DN used as the search base point

#: Register the settings defined for the `auth.server.name` key.

Related topics

- hcmds64ldapuser in the manual JP1/Automatic Operation Command and API Reference
- 2.8 Configuration file for external authentication server linkage (exauth.properties)

3.2.5 Checking JP1/AO connection with Active Directory

Execute the `hcmds64checkauth` command to confirm that JP1/AO can connect to Active Directory by using the information registered in the configuration file for external authentication server linkage (exauth.properties).

Related topics

- hcmds64checkauth in the manual JP1/Automatic Operation Command and API Reference

3.2.6 Registering user information in JP1/AO

If you do not link groups, users registered in Active Directory must also be registered in JP1/AO. Make sure that Active Directory user IDs match the JP1/AO user IDs. There is no need to set passwords.

Related topics

- Adding users to JP1/AO in the JP1/Automatic Operation Administration Guide

3.2.7 Assigning roles to Active Directory groups

If you link groups, use the **Add Groups** dialog box to register Active Directory groups as JP1/AO user groups. Then, assign service groups and roles to the registered user groups.

Related topics

- Creating Active Directory groups that link with JP1/AO in the JP1/Automatic Operation Administration Guide
- Assigning service groups and roles to user groups in the JP1/Automatic Operation Administration Guide

3.2.8 Security settings for communication with the LDAP directory server

Security settings are required when communicating using startTLS as the protocol for connecting to the LDAP directory server. You must use the `hcmds64keytool` command (for Windows) or the `keytool` command (for Linux) to import the SSL server certificate into the common component truststore.

> **Tip**
>
> You do not need to perform this procedure if you do not use startTLS as the protocol for connecting to the LDAP directory server.

Before you begin

- Use a secure method to acquire the SSL server certificate to be imported.
- Check the path of the SSL server certificate to be imported.
- Check the path of the truststore file.

  In Windows:

  Common-Component-installation-folder`\conf\sec\ldapcacerts`

  In Linux:

  Common-Component-installation-directory`/conf/sec/ldapcacerts`
- Check the access password for the truststore. If the truststore already exists, check the password you specified when you created it.
- The SSL server certificate you are importing must have the following conditions:
  - The format is PEM or DER.
  - The certificates of all certificate authorities from the certificate authority that issued the SSL server certificate of the LDAP directory server to the root certificate authority are chained.
  - The same host name as the CN of the SSL server certificate of the LDAP directory server is specified in "auth.ldap.*server-identifier*.host" in the Configuration file for external authentication server linkage.

Procedure to import SSL server certificate to truststore of Common Component

You can import an SSL server certificate into the truststore of the Common Component by executing a command. To import an SSL server certificate into the truststore of the Common Component:

1. Execute the following command:

   In Windows:

   Common-Component-installation-folder`\bin\hcmds64keytool -import -alias` *alias-name* `-file` *SSL-server-certificate-path* `-keystore` *truststore-file-path* `-storepass` *truststore-accesspassword*

   In Linux 6, Linux 7, SUSE Linux 12:

   Common-Component-installation-directory`/uCPSB/jdk/bin/keytool -import -alias` *alias-name* `-file` *SSL-server-certificate-path* `-keystore` *truststore-file-path* `-storepass` *truststore-accesspassword*

In Linux 8:

Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -import -alias *alias-name* -file *SSL-server-certificate-path* -keystore *truststore-file-path* -storepass *truststore-accesspassword* -storetype JKS

Important

Note the following points when you specify *alias-name*, *truststore-file-path*, and *truststore-accesspassword* by using the hcmds64keytool or keytool command:

- For *alias-name*, specify the name used to identify the certificate within the truststore. If there are multiple SSL server certificates, specify an alias that is not already in use in the truststore.
- The following symbols cannot be used in *truststore-file-path*:
  Colons (:), commas (,), semicolons (;), asterisks (*), question marks (?), double quotation marks ("), left and right angle brackets (< and>), vertical bars (|), and hyphens (-)
- Specify *truststore-file-path* as a character string of 255 bytes or fewer.
- Double quotation marks (") cannot be used in *alias-name* or *truststore-access-password*.

2. Restart the JP1/AO server.

Procedure to check SSL server certificate of truststore of Common Component

You can see the SSL server certificate imported into the common component truststore with the following command:

In Windows:

Common-Component-installation-folder\bin\hcmds64keytool -list -v -keystore *truststore-file-path* -storepass *truststore-accesspassword*

In Linux 6, Linux 7, SUSE Linux 12:

Common-Component-installation-directory/uCPSB/jdk/bin/keytool -list -v -keystore *truststore-file-path* -storepass *truststore-accesspassword*

In Linux 8:

Common-Component-installation-directory/uCPSB11/jdk/bin/keytool -list -v -keystore *truststore-file-path* -storepass *truststore-accesspassword*

Procedure to delete SSL server certificate imported into truststore of Common Component

You can delete an SSL server certificate imported into the truststore of the Common Component by executing a command. To delete an SSL server certificate imported into the truststore of the Common Component:

1. Execute the following command:

   In Windows:

   Common-Component-installation-folder\bin\hcmds64keytool -delete -alias *alias-name* -keystore *truststore-file-path* -storepass *truststore-accesspassword*

   In Linux 6, Linux 7, SUSE Linux 12

   Common-Component-installation-directory/uCPSB/jdk/bin/keytool -delete -alias *alias-name* -keystore *truststore-file-path* -storepass *truststore-accesspassword*

In Linux 8:

Common-Component-installation-directory`/uCPSB11/jdk/bin/keytool -delete -alias` *alias-name* `-keystore` *truststore-file-path* `-storepass` *truststore-accesspassword*

2. Restart the JP1/AO server.

3.3 Linking to the JP1/IM event monitoring function

3.3.1 Procedure for linking to the JP1/IM event monitoring function

By linking to the JP1/IM event monitoring function, you will be able to centrally monitor JP1 events by using JP1/IM.

Before you begin

Check the prerequisites for linking to JP1/IM.

To link to the JP1/IM event monitoring function:

1. Edit the integrated function menu definition file.
2. Copy the definition file for object types, the definition file for the extended event attributes, the definition file for opening monitor windows, and the integrated function menu definition file to the JP1/IM - Manager and JP1/IM - View folders.

   Note: These definition files are coded for a Windows environment. To copy these definition files to JP1/IM in a Linux environment, you must first change the character encoding to UTF-8 and the line break code to LF by using a text editor, the `nkf` command, or another means.
3. To enable the definition files, restart JP1/IM.
4. Make sure that notification of JP1 events is enabled.

   If the notification.jp1event key in the user-specified properties file (config_user.properties) is set to `true`, notification of JP1 events is enabled.

Related topics

- Configuration for linking with JP1/IM - Manager in the JP1/Automatic Operation Overview and System Design Guide
- 3.3.2 Definition files used for linking to JP1/IM
- 3.3.3 Integrated function menu definition file (hitachi_jp1_ao_tree.conf)
- 3.3.4 Target folders into which definition files for linking to JP1/IM (in a Windows environment) are copied
- 3.3.5 Target directories into which definition files for linking to JP1/IM (for a UNIX environment) are copied
- 2.2 User-specified properties file (config_user.properties)

3.3.2 Definition files used for linking to JP1/IM

To link to JP1/IM, use the integrated function menu definition file, the definition file for object types, the definition file for the extended event attributes, and the definition file for opening monitor windows.

In the integrated function menu definition file, you need to edit the section where the JP1/AO server host name, port number, and similar information is defined.

Installation folder

Integrated function menu definition file

For non-cluster systems:

JP1/AO-installation-folder\conf\event\jp1imview or /opt/jp1ao/conf/event/jp1imview

For cluster systems:

shared-folder-name\jp1ao\conf\event\jp1imview or *shared-folder-name*/jp1ao/conf/event/jp1imview

Definition file for object types, Definition file for the extended event attributes and Definition file for opening monitor windows

For non-cluster systems:

JP1/AO-installation-folder\conf\event\jp1imm or /opt/jp1ao/conf/event/jp1imm

For cluster systems:

shared-folder-name\jp1ao\conf\event\jp1imm or *shared-folder-name*/jp1ao/conf/event/jp1imm

Table 3-8: Definition files used for linking to JP1/IM

Definition file	File name	Contents	Can edit
Integrated function menu definition file	Japanese environment: hitachi_jp1_ao_tree.conf# English environment: hitachi_jp1_ao_tree.conf# Chinese environment: hitachi_jp1_ao_tree.conf#	Defines information for displaying trees in the **Tool Launcher** window of JP1/IM - View.	Y
Definition file for object types	Japanese environment: hitachi_jp1_ao_obj.ja# English environment: hitachi_jp1_ao_obj.en# Chinese environment: hitachi_jp1_ao_obj.zh#	Defines items displayed in **Object type** and **Root object type** in the **Severe Event Definition** window and **Event Acquisition Settings** window in JP1/IM - View.	N
Definition file for the extended event attributes	Japanese environment: hitachi_jp1_ao_attr_sys_ja.conf# English environment: hitachi_jp1_ao_attr_sys_en.conf# Chinese environment: hitachi_jp1_ao_attr_sys_zh.conf#	Defines the displayed attribute names and the order of event attributes to display in the **Event Details** window of JP1/IM - View. The specifics of the extended event attributes are defined in this definition file.	N
Definition file for opening monitor windows	Japanese environment: hitachi_jp1_ao_mon_sys_alarm_ja.conf# English environment: hitachi_jp1_ao_mon_sys_alarm_en.conf# Chinese environment: hitachi_jp1_ao_mon_sys_alarm_zh.conf#	Defines information for opening monitor windows from the **Event Console** window in JP1/IM - View to display the event issuer and similar information.	N

Legend:

Y: Can be edited. N: Cannot be edited.

#

These definition files are stored in the appropriate folders for each language.

Related topics

- 3.3.1 Procedure for linking to the JP1/IM event monitoring function
- 3.3.3 Integrated function menu definition file (hitachi_jp1_ao_tree.conf)

3.3.3 Integrated function menu definition file (hitachi_jp1_ao_tree.conf)

This is the definition file that must be edited for linking to the event monitoring function of JP1/IM.

It defines information for displaying trees in the **Tool Launcher** window of JP1/IM - View.

Format

specification-key-name=setting

Installation folder

For non-cluster systems:

Japanese environment:
JP1/AO-installation-folder\conf\event\jp1imview\ja or /opt/jp1ao/conf/event/jp1imview/ja

English environment:
JP1/AO-installation-folder\conf\event\jp1imview\en or /opt/jp1ao/conf/event/jp1imview/en

Chinese environment:
JP1/AO-installation-folder\conf\event\jp1imview\zh or /opt/jp1ao/conf/event/jp1imview/zh

For cluster systems:

Japanese environment:
shared-folder-name\jp1ao\conf\event\jp1imview\ja or *shared-folder-name*/jp1ao/conf/event/jp1imview/ja

English environment:
shared-folder-name\jp1ao\conf\event\jp1imview\en or *shared-folder-name*/jp1ao/conf/event/jp1imview/en

Chinese environment:
shared-folder-name\jp1ao\conf\event\jp1imview\zh or *shared-folder-name*/jp1ao/conf/event/jp1imview/zh

Trigger for applying definitions

Restarting the service (JP1/IM)

Description

In the integrated function menu definition file, the <JP1_AO_HOST> block specifies the host name or IP address of the JP1/AO server, and the <PORT_NO> block specifies the port number for the terminals that use JP1/AO.

To launch Web interfaces to JP1/AO on different servers, you must define a block for each server in the integrated function menu definition file.

Example definitions

Example of HTTP connection to Web server with JP1/AO host name AO-Host and port number 22015:

```
#All Rights Reserved. Copyright (C) 2012, Hitachi, Ltd.
#Licensed Material of Hitachi, Ltd.

#Comment Declaration that this is the integrated function menu definition file
@file type="function-definition", version="0300";

#Comment Function tree menu definition block - folder
@define-block type="function-tree-def";
id="jco_folder_ AutomaticOperation";
parent_id="root";
name="IT operation automation";
@define-block-end;

#Comment Function tree menu definition block-tier1
@define-block type="function-tree-def";
id="jco_JP1_AO";
parent_id="jco_folder_ AutomaticOperation";
name="IT operation automation platform";
execute_id="default_browser";
arguments="http://AO-Host:22015/Automation/launcher/Login?jp1token=%JCO_JP1TOKEN$E
NC$URLENC%";
```

Example of configuring two servers in the integrated function menu definition file:

```
#All Rights Reserved. Copyright (C) 2012, Hitachi, Ltd.
#Licensed Material of Hitachi, Ltd.

#Comment Declaration that this is the integrated function menu definition file
@file type="function-definition", version="0300";

#Comment Function tree menu definition block - folder
@define-block type="function-tree-def";
id="jco_folder_ AutomaticOperation";
parent_id="root";
name="IT operation automation";
@define-block-end;

#Comment Function tree menu definition block-tier1
@define-block type="function-tree-def";
id="jco_JP1_AO1";
parent_id="jco_folder_ AutomaticOperation";
name="IT operation automation platform 01";
execute_id="default_browser";
arguments="http://AO-Host:22015/Automation/launcher/Login?jp1token=%JCO_JP1TOKEN$E
NC$URLENC%";
@define-block-end;
#------------------------------------------------------------------------------
@define-block type="function-tree-def";
id="jco_JP1_AO2";
parent_id="jco_folder_ AutomaticOperation";
name="IT operation automation platform 02";
execute_id="default_browser";
arguments="http://AO-Host:22015/Automation/launcher/Login?jp1token=%JCO_JP1TOKEN$E
NC$URLENC%";
@define-block-end;
```

Related topics

- 3.3.1 Procedure for linking to the JP1/IM event monitoring function
- Evaluating the system configuration in the JP1/Automatic Operation Overview and System Design Guide

3.3.4 Target folders into which definition files for linking to JP1/IM (in a Windows environment) are copied

After editing the definition files for linking to JP1/IM, copy them to the JP1/IM - Manager and JP1/IM - View folders.

The target folders into which to copy the files to are different depending on whether a physical host or a logical host is configured.

Table 3-9: Where to copy definition files for linking to JP1/IM (Windows)

Definition file	Folder to copy it to
Integrated function menu definition file	Japanese environment: *JP1/IM-View-installation-folder*\JP1CoView\conf\function\ja English environment: *JP1/IM-View-installation-folder*\JP1CoView\conf\function\en Chinese environment: *JP1/IM-View-installation-folder*\JP1CoView\conf\function\zh
Definition file for object types	Physical host: *JP1/IM-Manager-installation-folder*\JP1Cons\conf\console\object_type Logical host: *shared-folder-name*\jp1cons\conf\console\object_type
Definition file for the extended event attributes	Physical host: *JP1/IM-Manager-installation-folder*\JP1Cons\conf\console\attribute Logical host: *shared-folder-name*\jp1cons\conf\console\attribute
Definition file for opening monitor windows	Physical host: *JP1/IM-Manager-installation-folder*\JP1Cons\conf\console\monitor Logical host: *shared-folder-name*\jp1cons\conf\console\monitor

Related topics

- 3.3.1 Procedure for linking to the JP1/IM event monitoring function

3.3.5 Target directories into which definition files for linking to JP1/IM (for a UNIX environment) are copied

After editing the definition files for linking to JP1/IM, copy them to the JP1/IM - Manager directories.

The target directories into which to copy the files are different depending on whether a physical host or a logical host is configured.

Table 3-10: Where to copy definition files for linking to JP1/IM (UNIX)

Definition file	Directory to copy it to
Integrated function menu definition file	(No need to copy in UNIX)
Definition file for object types	Physical host: /etc/opt/jp1cons/conf/console/object_type Logical host: *shared-directory*/jp1cons/conf/console/object_type
Definition file for the extended event attributes	Physical host: /etc/opt/jp1cons/conf/console/attribute Logical host: *shared-directory*/jp1cons/conf/console/attribute
Definition file for opening monitor windows	Physical host: /etc/opt/jp1cons/conf/console/monitor Logical host: *shared-directory*/jp1cons/conf/console/monitor

Related topics

- 3.3.1 Procedure for linking to the JP1/IM event monitoring function

4 Changing System Information

This chapter describes how to change settings related to the JP1/AO system, including items that were set during JP1/AO installation.

4.1 Procedure to change the JP1/AO installation folder

To change the installation folder, uninstall JP1/AO, and then re-install it. Note that if the OS of the JP1/AO server is Linux, you cannot change the installation folder.

In other cases, although you can change the installation folder, if you change it, you cannot recover the definitions in the user-specified properties file (config_user.properties) from a backup. You must re-set the definitions after reinstalling JP1/AO.

Related topics

- 1.3.3 Installation folder for each product
- 7.1 Uninstallation procedure
- 1.1 New installation procedure
- 2.2 User-specified properties file (config_user.properties)

4.2 Procedure to change the database installation folder

To change the database installation folder, you must uninstall JP1/AO, and then re-install it. Note that if the OS of the JP1/AO server is Linux, you cannot change the database installation folder.

In other cases, although you can change the database installation folder, if you change it, you cannot recover the definitions in the user-specified properties file (config_user.properties) from a backup. You must re-set the definitions after reinstalling JP1/AO.

Related topics

- 1.3.4 Installation folders for databases
- 7.1 Uninstallation procedure
- 1.1 New installation procedure
- 2.2 User-specified properties file (config_user.properties)

4.3 Procedure to change the host name of the JP1/AO server

4.3.1 Procedure to change the host name of the JP1/AO server (non-cluster system)

If JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products are installed, you need to change the settings in JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products at the same time. For details, see the manuals for JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products.

To change the host name of the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Edit the user_httpsd.conf file to change the value of the ServerName directive to the new host name.

   The user_httpsd.conf file is stored in the following folder:

   - If the OS of the JP1/AO server is Windows
     Common-Component-installation-folder`\uCPSB\httpsd\conf`
   - If the OS of the JP1/AO server is Linux 6, Linux 7, SUSE Linux 12
     `/opt/HiCommand/Base64/uCPSB/httpsd/conf`
   - If the OS of the JP1/AO server is Linux 8
     `/opt/HiCommand/Base64/uCPSB11/httpsd/conf`

   If HTTPS connections are enabled, re-obtain the SSL server certificate and change the value of the ServerName directive in the VirtualHost directive to the new host name.
3. Restart the JP1/AO server.
4. Execute the `hcmds64chgurl` command to update the URL.

Related topics

- 4.6 Procedure to change the URL

4.3.2 Procedure to change the host name of the JP1/AO server (cluster system)

For a cluster system, the host name of the logical host can be changed, but not the host name of the physical host.

If JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products are installed, you need to change the settings in JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products at the same time. For details, see the manuals for JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products.

Before you begin

Log in to the JP1/AO server as a user who has not only administrator or root permissions on the OS, but also administrator permissions on the cluster.

To change the host name of the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
3. Use the cluster software to bring the above resource group online.
4. Use the cluster software to take services other than the HiRDB/ClusterService _HD1 service and scripts offline.
5. On the active server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
6. Use the cluster software to bring the service (HiRDB/ClusterService _HD1) offline.
7. In the cluster software, suppress failover for the resource group where JP1/AO services and scripts is registered.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart does not occur if the resource fails. Perform this action for all services and scripts registered in the resource group in order to suppress failover.
8. In the cluster software, change the logical host name (client access point) of the resource group in which JP1/AO is registered.
9. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
10. On the active server, modify the cluster settings file (*Common-Component-installation-folder*¥conf¥cluster.conf).

    For details, see 5.5 Cluster settings file (cluster.conf).
11. On the active server, edit the user_httpsd.conf file to change the value of the ServerName directive to the new host name.

    The user_httpsd.conf file is stored in the following folder:

    - If the OS of the JP1/AO server is Windows

      Common-Component-installation-folder`\uCPSB\httpsd\conf`
    - If the OS of the JP1/AO server is Linux 6, Linux 7, SUSE Linux 12

      `/opt/HiCommand/Base64/uCPSB/httpsd/conf`
    - If the OS of the JP1/AO server is Linux 8

      `/opt/HiCommand/Base64/uCPSB11/httpsd/conf`

    If HTTPS connections are enabled, re-obtain the SSL server certificate and change the value of the ServerName directive in the VirtualHost directive to the new host name.
12. If the OS is Linux, on the active server, execute the `hcmds64srv` command with the `status` option specified to check the status of each service. If the database for the Common Component (HiRDB service) is not running, start the database by executing the `hcmds64dbsrv` command with the `start` option specified.
13. If the HAutomation Engine Web Service is running on the active server, stop it by executing the `hcmds64srv` command with the `/stop /server AutomationWebService` option specified.
14. Execute the `setupcluster` command on the active server.
15. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
16. On the standby server, create a cluster settings file (*Common-Component-installation-folder*¥conf¥cluster.conf).

    For details, see 5.5 Cluster settings file (cluster.conf).
17. On the standby server, edit the user_httpsd.conf file to change the value of the ServerName directive to the new host name.

    The user_httpsd.conf file is stored in the following folder:

- If the OS of the JP1/AO server is Windows
  Common-Component-installation-folder\uCPSB\httpsd\conf
- If the OS of the JP1/AO server is Linux 6, Linux 7, SUSE Linux 12
  /opt/HiCommand/Base64/uCPSB/httpsd/conf
- If the OS of the JP1/AO server is Linux 8
  /opt/HiCommand/Base64/uCPSB11/httpsd/conf

If HTTPS connections are enabled, re-obtain the SSL server certificate and change the value of the ServerName directive in the VirtualHost directive to the new host name.

18. If the OS is Linux, on the standby server, execute the hcmds64srv command with the status option specified to check the status of each service. If the database for the Common Component (HiRDB service) is not running, start the database by executing the hcmds64dbsrv command with the start option specified.
19. If the HAutomation Engine Web Service is running on the standby server, stop it by executing the hcmds64srv command with the /stop /server AutomationWebService option specified.
20. Execute the setupcluster command on the standby server.
21. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
22. Use the cluster software to enable failover of the resource group where JP1/AO services and scripts is registered.
    Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if the resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.
23. Bring the resource group online by using the cluster software.

4.4 Procedure to change the IP address of the JP1/AO server

4.4.1 Procedure to change the IP address of the JP1/AO server (non-cluster system)

To change the IP address of the JP1/AO server, you must stop and restart the JP1/AO service.

The procedure to change the IP address is the same for both IPv4 and IPv6.

To change the IP address of the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in the execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Execute the `hcmds64srv` command with the `stop` option specified to stop the JP1/AO service.
3. Change the IP address of the JP1/AO server.
4. Execute the `hcmds64srv` command with the `start` option specified to start the JP1/AO service.

4.4.2 Procedure to change the IP address of the JP1/AO server (cluster system)

To change the IP address of the JP1/AO server, you must bring the resource group offline where the JP1/AO service is registered and stop the service.

The procedure to change the IP address is the same for both IPv4 and IPv6.

Before you begin

Log in to the JP1/AO server as a user who has not only the administrator or root permissions on the OS, but also administrator permissions on the cluster.

To change the IP address of the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. On the active server, use the cluster software to bring the resource group offline where the JP1/AO service is registered.
3. Change the IP address of the JP1/AO server
4. On the active server, use the cluster software to bring the resource group online where the JP1/AO service is registered.

4.5 Procedure to change the port number

4.5.1 Procedure to change the port number used for communications between JP1/AO and Web browsers

To change the port number used for communications between JP1/AO and Web browsers, you must edit the definition file and register exceptions in the firewall.

For a cluster system, perform the same procedure on both the active server and the standby server.

Before you begin

Make sure that there are no tasks that are waiting or running in JP1/AO.

In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.

To change the port number between JP1/AO and Web browsers (if the communication protocol is HTTP):

1. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `stop` option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.

2. Change the port number settings by editing the keys in the definition files as follows:

   - `Listen` in *Common-Component-installation-folder*`\uCPSB\httpsd\conf\user_httpsd.conf` (in Windows), `/opt/HiCommand/Base64/uCPSB/httpsd/conf/user_httpsd.conf` (in Linux 6, Linux 7, SUSE Linux 12), or `/opt/HiCommand/Base64/uCPSB11/httpsd/conf/user_httpsd.conf` (in Linux 8)

     Specify the new number in place of 22015 on the following lines:

     ```
     Listen [::]:22015
     Listen 22015
     ```

     In a cluster system, specify the same settings on both the active server and the standby server.

   - command.http.port in command_user.properties

     The folder that contains the above definition file is different for non-cluster systems and cluster systems.

     For non-cluster systems:

     JP1/AO-installation-folder`\conf` or `/opt/jp1ao/conf`

     For cluster systems:

     shared-folder-name`\jp1ao\conf` or *shared-folder-name*`/jp1ao/conf`

   - server.http.port in config_user.properties

     The folder that contains the above definition file is different for non-cluster systems and cluster systems.

     For non-cluster systems:

     JP1/AO-installation-folder`\conf` or `/opt/jp1ao/conf`

For cluster systems:

shared-folder-name\jp1ao\conf or *shared-folder-name*/jp1ao/conf

3. If the OS is Windows, execute the hcmds64fwcancel command to register exceptions in the firewall.

   If the OS is Linux, register exceptions according to OS specifications. For details about the procedure, see the documentation for the OS.

   In a cluster system, perform this step on both the active server and the standby server.

4. Start the JP1/AO service.

   For non-cluster systems:

   Execute the hcmds64srv command with the start option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

5. Execute the hcmds64chgurl command to update the URL.

6. If the OS of the JP1/AO server is Windows, change the port number in the URL of the shortcut file to the page displayed by performing the following operation:

   From the Start menu, select **All Program**, **JP1_Automatic Operation**, and then **JP1_AO Login**.

To change the port number between JP1/AO and Web browsers (if the communication protocol is HTTPS):

1. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the hcmds64srv command with the stop option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.

2. Change the port number settings by editing the keys in the definition files as follows:

   Listen and VirtualHost *host-name*:*port* in *Common-Component-installation-folder*\uCPSB\httpsd\conf\user_httpsd.conf (in Windows), /opt/HiCommand/Base64/uCPSB/httpsd/conf/user_httpsd.conf (in Linux 6, Linux 7, SUSE Linux 12), or /opt/HiCommand/Base64/uCPSB11/httpsd/conf/user_httpsd.conf (in Linux 8)

   Specify the new number in the place of 22016 on the following lines:

   ```
   Listen [::]:22016
   Listen 22016
   <VirtualHost *:22016>
   ```

3. If the OS is Windows, execute the hcmds64fwcancel command to register exceptions in the firewall.

   If the OS is Linux, register exceptions according to OS specifications. For details about the procedure, see the documentation for the OS.

   In a cluster system, perform this step on both the active server and the standby server.

4. Start the JP1/AO service.

   For non-cluster systems:

   Execute the hcmds64srv command with the start option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

5. Execute the hcmds64chgurl command to update the URL.

6. If the OS of the JP1/AO server is Windows, change the port number in the URL of the shortcut file to the page displayed by performing the following operation:
   From the Start menu, select **All Program**, **JP1_Automatic Operation**, and then **JP1_AO Login**.

Notes:

- If JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products are installed, the port number of JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products also changes. For details, see the manual of JP1/OA, Hitachi Command Suite products, or Hitachi Ops Center products.
- If you are using JP1/IM monitor startup and you perform a monitor startup of JP1 events before the port number is changed, the monitor startup fails.

Related topics

- JP/AO services in the JP1/Automatic Operation Administration Guide
- Login window in the JP1/Automatic Operation Administration Guide
- 4.6 Procedure to change the URL

4.5.2 Procedure to change the port number between JP1/AO and the SMTP server

You can change the port number used for communications between JP1/AO and the SMTP server in the **System Settings** area.

To change the port number between JP1/AO and the SMTP server:

1. In the **Administration** area of the **Administration** window, select the **System Settings** menu.
2. In the **System Settings** area, click the **Edit** button.
3. Enter the new port number and then click the **OK** button.

Related topics

- List of shared built-in service properties in the JP1/Automatic Operation Administration Guide

4.5.3 Procedure to change the SSH or Telnet port number used for communications between JP1/AO and operation target devices

To change the port number used for communications between JP1/AO and operation target devices, you must edit the definition file and register exceptions in the firewall.

Before you begin

Make sure that there are no tasks waiting or running in JP1/AO. In the **Tasks** window, check the tasks.

If any tasks are in an execution status (In Progress, Waiting for Input, In Progress (with Error), Terminated, or Long Running), stop the execution of those tasks or wait until the task statuses change to the ended status.

To change the SSH or Telnet port number between JP1/AO and operation target devices:

1. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the stop option specified.

   For cluster systems:

   Use the cluster software to take the service offline.

2. Change the port number by editing the following key in the definition file:

   - To change the SSH port number: ssh.port.number in config_user.properties
   - To change the Telnet port number: telnet.port.number in config_user.properties

   The folder that contains the above definition file is different for non-cluster systems and cluster systems.

   For non-cluster systems:

   JP1/AO-installation-folder\conf or /opt/jp1ao/conf

   For cluster systems:

   shared-folder-name\jp1ao\conf or *shared-folder-name*/jp1ao/conf

3. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the start option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

Tip

To specify the SSH or Telnet port number for each operation target device, use the connection-destination property file (*connection-destination-name*.properties) to specify it.

Related topics

- 2.2 User-specified properties file (config_user.properties)

4.5.4 Procedure to change the port number between JP1/AO and the LDAP directory server

To change the port number between JP1/AO and the LDAP directory server, you must edit the definition file and register exceptions in the firewall.

In a cluster system, perform the same procedure on both the active server and the standby server.

Before you begin

Make sure that no user is logged in to the JP1/AO window.

To change the port number between JP1/AO and the LDAP directory server:

1. Change the port number by editing the following key of the definition file:
   auth.ldap.*server-identifier*.port (see Note) in exauth.properties

   Notes:

   For *server-identifier*, specify the same value specified for server-identifier for auth.server.name. The definition file is stored in the following folder:
   common-component-installation-folder\conf or /opt/HiCommand/Base64/conf

Related topics

- 2.8 Configuration file for external authentication server linkage (exauth.properties)

4.6 Procedure to change the URL

If you change the host name or IP address of the JP1/AO server or the port number used for communications between JP1/AO and the Web browser, you also need to change the URL by using the `hcmds64chgurl` command.

To change the URL:

The following examples show the steps for changing the URL from http://192.168.11.33:22015 to http://192.168.11.55:22015.

1. Execute the `hcmds64chgurl` command with the `list` option specified to find the currently registered URL.

   Example in Windows:

   ```
   hcmds64chgurl /list
   http://192.168.11.33:22015
   JP1/Automatic Operation
   ```

2. Execute the `hcmds64chgurl` command with the `change` option specified to update the URL.

   Example in Windows:

   ```
   hcmds64chgurl /change "http://192.168.11.33:22015" "http://192.168.11.55:22015"
   The URL was changed from "http://192.168.11.33:22015" to "http://192.168.11.55:2
   2015".
   ```

3. Execute the `hcmds64chgurl` command with the `list` option specified to confirm that the URL has been updated.

   Example in Windows:

   ```
   hcmds64chgurl /list
   http://192.168.11.55:22015
   JP1/Automatic Operation
   ```

4.7 Procedures to change the time on the JP1/AO server

4.7.1 Procedure to move the time forward on the JP1/AO server

To move the time forward on the JP1/AO server, you must restart the product.

In a cluster system, change the time on both the active server and the standby server. For the procedures to start and stop the JP1/AO system, follow the instructions in the *JP1/Automatic Operation Administration Guide*.

To move the time forward on the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in the execution status (In Progress, Waiting for Response, Abnormal Detection, Terminated, or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `stop` option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.
3. Move the time forward on the JP1/AO server.
4. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `start` option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

Related topics

- JP/AO services in the JP1/Automatic Operation Administration Guide

4.7.2 Procedure to move the time back on the JP1/AO server

To move the time back on the JP1/AO server, you must restart the product.

In a cluster system, change the time on both the active server and the standby server. For the procedures to start and stop the JP1/AO system, follow the instructions in the *JP1/Automatic Operation Administration Guide*.

To move the time back on the JP1/AO server:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `stop` option specified.

For cluster systems:

Use the cluster software to bring the service offline.

3. Note the current time indicated on the JP1/AO server.
4. Move the time back on the JP1/AO server.
5. Wait until the time you noted in step 4 is reached, and then start the service.

For non-cluster systems:

Execute the `hcmds64srv` command with the `start` option specified.

For cluster systems:

Use the cluster software to bring the service online.

If you use NTP to automatically correct the time, do not allow it to correct the server time retroactively when the time indicated on the server is ahead of the actual time. In the NTP function for correcting the time automatically, if the time difference falls within a predetermined range, the time is adjusted incrementally, whereas if it exceeds that range, the time is adjusted retroactively all at once. Set the frequency of time adjustments in such a way that the time difference will not exceed the range within which the time can be adjusted incrementally.

Related topics

- JP/AO services in the JP1/Automatic Operation Administration Guide

4.8 Procedure to change the maximum number of plug-ins that can be executed concurrently

To change the maximum number of plug-ins that can be executed concurrently, you must restart the product.

You can change the maximum number of concurrently executable plug-ins that are included in normal tasks. The value that can be specified is 10, 50, or 100.

If you change the maximum number of plug-ins that can be executed concurrently, you must also review the amount of memory on the JP1/AO server.

To change the maximum number of plug-ins that can be executed concurrently:

1. Estimate the maximum number of plug-ins that will be executed concurrently. Then, based on this estimation, secure the necessary amount of memory on the JP1/AO server. The following table lists the relationship between the number of concurrently executed plug-ins and the amount of memory required on the JP1/AO server.

   Table 4-1: Relationship between the number of concurrently executed plug-ins and the amount of memory required on the JP1/AO server

Number of concurrently executed plug-ins	Amount of memory required on the JP1/AO server (GB)#	
	Minimum	Recommended
10	4	6
50	5	7
100	6	8

   # If the upper limit values for the following types of processing might be reached at the same time, we recommend that you secure the *recommended* amount of memory:

   - User-response wait plug-ins (upper limit: 70)
   - Repeated execution plug-ins (upper limit: 20)
   - Debug tasks (upper limit: 10)

2. For the `plugin.threadPoolSize` key in the user-specified properties file (config_user.properties), specify the *number-of-concurrently-executed-plug-ins* value (10, 50, or 100) in the following format:

   `plugin.threadPoolSize =` *number-of-concurrently-executed-plug-ins*

3. Stop the JP1/AO services.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `stop` option specified.

   For cluster systems:

   Use the cluster software to bring the services offline.

4. Start the JP1/AO services.

   For non-cluster systems:

   Execute the `hcmds64srv` command with the `start` option specified.

   For cluster systems:

   Use the cluster software to bring the services online.

Tip

When plug-ins requiring a long execution time are executed concurrently, if the maximum number of concurrently executable plug-ins is reached, other plug-ins are placed in a wait state and cannot start even if the system has sufficient processing performance. In such a case, you can reduce unnecessary waits to shorten the overall processing time by increasing the maximum number of concurrently executable plug-ins. Note that you cannot shorten the processing time by this method in cases requiring all JP1/AO processing ability, such as when many plug-ins requiring a short execution time are executed.

Related topics

- 2.2 User-specified properties file (config_user.properties)

5 Setting up a cluster system

This chapter describes how to set up a JP1/AO cluster system.

5.1 Procedure for installing JP1/AO in a cluster system

After checking the prerequisites, install JP1/AO in both the active server and standby server.

To install JP1/AO in a cluster system, perform the procedure described below.

Table 5-1: Procedure for installing JP1/AO in a cluster system

Task		Required/ optional	Reference
1	Check the installation prerequisites.	Required	5.2 Installation prerequisites (for cluster systems)
2	Install JP1/AO.	Required	The reference depends on the current environment and the installation status of the product.#
3	Install the manual on the JP1/AO server.	Optional	1.4 Procedure to install the manual
4	Install JP1/AO Content Pack.	Optional	1.5 Installing JP1/AO Content Pack

#

The procedure for installing JP1/AO differs depending on the current configuration of the environment and on whether products have been installed.

Table 5-2: Possible environments when setting up a cluster system

Current environment	JP1/AO installation status	Common Component installation status	Reference
Cluster system set up	Y	Y	6.5 Procedure to perform an overwrite or upgrade installation of JP1/AO (for a Windows cluster system)
	N	Y	5.4 Installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)
		N	5.3 Installing JP1/AO in a cluster system
Cluster system not set up	N	Y	
		N	

Legend:

Y: installed N: not installed

Note that cluster systems built in either of the following ways are not supported:

- A non-cluster environment in which JP1/AO is already operating is rebuilt in a cluster configuration later.
- A Linux cluster system is newly built in an environment in which Common Component has already been installed.

5.2 Installation prerequisites (for cluster systems)

Before installing JP1/AO in a cluster system, you must check and prepare the installation environment.

- Conflicting products

  Before you start installation of JP1/AO, uninstall the following conflicting products:

  - Hitachi Automation Director
  - Hitachi Command Suite products (if the OS of the JP1/AO server is Linux)
- OS

  Patches and service packs required by JP1/AO and the cluster software must have been installed.

  For the latest information about the prerequisite OSs, see the *Release Notes*.
- Configuration
  - The environment of each server must be the same so that the same processing can be performed in the event of failover.
  - The cluster must be configured with two or more servers.
- Disk

  Files must be protected by a method such as a journaling file system so that data will not be lost in the event of a system shutdown.
- Network
  - Communication must be possible by using the IP address that corresponds to the host name (result of execution of the `hostname` command). It must not be possible for a program such as the cluster software to set a status that disables communication.
  - The correspondence between the host name and the IP address cannot be changed while JP1/AO is operating. It must not be possible for programs, such as the cluster software and name server, to change the correspondence.
  - The LAN board corresponding to the host name must have the highest priority in the network bind settings. Priority must not be given to any other LAN board, including a heartbeat LAN board.
- DNS operation

  Host names must be entered without the domain name. FQDN-format host names cannot be used.
- Shared disk

  To prevent data corruption on the active server in the event of failover, make sure that all the conditions listed below have been met. If the conditions are not met, problems might occur that prevent JP1/AO from working properly, including errors, data loss, and failure to start.
  - JP1/AO must not be installed on the shared disk.
  - A shared disk that can be carried over from the active server to the standby server must be available.
  - The shared disk must have been allocated before JP1/AO was started.
  - Allocation of the shared disk cannot be released during JP1/AO execution.
  - Allocation of the shared disk must be released after JP1/AO has stopped.
  - The shared disk must be locked so that it will not be accessed improperly by multiple servers.
  - Files must be protected by a method such as a journaling file system so that data will not be lost in the event of a system shutdown.
  - The contents of files must be protected and inherited in the event of a failover.

- Forced failover must be available in the event that the shared disk is being used by a process at the time of a failover.
- If JP1/AO needs to be started or stopped as part of the recovery process when failure is detected on the shared disk, you must be able to start or stop JP1/AO from the cluster software.

- Logical host name, IP address

  Check the conditions below so that recovery actions can be performed in the event of failure in a LAN board. If the conditions are not met, communication errors will prevent JP1/AO from working correctly until the LAN boards are swapped or failover to another server is achieved by the cluster software or some other means.

  - The name of the logical host must be 32 bytes or less.
  - Characters other than alphanumeric characters and hyphens (-) must not be used in the host name.
  - Inheritable logical IP addresses must be available for communications.
  - It must be possible for a unique logical IP address to be obtained from the logical host name.
  - The logical host names must be set in the hosts file or name server, and must be reachable via TCP/IP communication.
  - The logical IP addresses must be assigned before JP1/AO starts.
  - The logical IP addresses cannot be deleted during JP1/AO execution.
  - The correspondence between the logical host name and the logical IP address cannot change during JP1/AO execution.
  - The logical IP addresses must not be deleted until after JP1/AO has stopped.
  - In the event of a network failure, the cluster software must be able to manage the recovery process so that JP1/AO does not have to handle the recovery. If JP1/AO needs to be started or stopped as part of the recovery process, the cluster software must issue the start or stop request to JP1/AO.

- Port numbers

  The port number for connecting to the Web server must be the same in both the active server and the standby server. If the port numbers are not the same, the JP1/AO operations window will not be displayed in the Web browser when the servers are swapped at failover. If you change the port number, make sure that the new port number is the same on both the active server and standby server.

  Before installing JP1/AO on Linux 8, you must verify that port numbers 22170 - 22173 are not used by other products on JP1/AO server.

5.3 Installing JP1/AO in a cluster system

To set up a cluster system, you must install JP1/AO on both the active server and standby server.

When you set up JP1/AO in a cluster system, it also sets up Common Component, which is used by Hitachi Command Suite products.

To install JP1/AO, perform the procedure described below.

Table 5-3: Procedure for installing JP1/AO in a cluster system

Task		Required/ optional	Reference
1	Perform the tasks that must be completed in advance.	Required	5.3.1 Tasks required before installation of JP1/AO in a cluster system
2	Create a resource group by using the cluster software.	Required	5.3.2 Procedure for creating a resource group by using the cluster software
3	Install JP1/AO on the active server and standby server.	Required	5.3.3 Procedures for installing JP1/AO on the active server and standby server
4	Set up the active server.	Required	5.3.4 Procedure for setting up the active server
5	Set up the standby server.	Required	5.3.5 Procedure for setting up the standby server
6	If the OS is Windows, register services in the cluster software.	Required	5.3.6 Procedure for using the cluster software to register services (in Windows)
	If the OS is Linux, register services and configure a resource group in the cluster software.	Required	5.3.7 Procedure for using the cluster software to register resources and to set up the resource group (in Linux)

Related topics

- 5.2 Installation prerequisites (for cluster systems)

5.3.1 Tasks required before installation of JP1/AO in a cluster system

Before you install JP1/AO in a cluster system, you must perform the tasks described below.

Before you begin

- Check the installation prerequisites (for cluster system).
- Log in to the JP1/AO server as a user who has not only administrator or root permissions on the OS, but also administrator permissions on the cluster.

5.3.2 Procedure for creating a resource group by using the cluster software

Create a resource group by using the cluster software.

To create a resource group by using the cluster software:

1. Install the cluster software on the active server and the standby server, and then set up the cluster system.
   - Install the cluster software according to the procedure specified by the OS.
   - Create the cluster by using the cluster software.
2. Create a resource group by using the cluster software.

   A resource group is a collection of services to be clustered together and treated as a unit for purposes of service failover.
   - Register the shared disk used in JP1/AO to the resource group of the cluster software.
   - If the OS is Windows, register the client access point to the resource group of the cluster software.

     For the network name, specify the logical host name used in JP1/AO. For the IP address, specify the logical IP address used in JP1/AO.
   - If the OS is Linux, register the logical host name and logical IP address used in JP1/AO to the resource group of the cluster software.

5.3.3 Procedures for installing JP1/AO on the active server and standby server

Install JP1/AO on both the active server and standby server.

To install JP1/AO on the active server and standby server:

1. Make sure that JP1/AO or any conflicting product is not installed on either the active or standby servers.

   If it is installed, uninstall JP1/AO or conflicting product.
2. Install JP1/AO on the active server.

   If the OS is Windows, perform the following operations:
   - Specify a path to a local disk for the location of the database.
   - Specify the physical host name for the JP1/AO server host name.
   - Specify a drive and folder as the installation destination. JP1/AO will be installed in the specified path on both the active and standby servers. If you see a message indicating that a restart is required after installation, restart the active server.

   If the OS is Linux, you do not need to specify the installation destination. JP1/AO will be installed at a fixed path on the local disk.
3. Install JP1/AO on the standby server.

   If the OS is Windows, perform the following operations:
   - Specify a path to a local disk for the location of the database.
   - Specify the physical host name for the JP1/AO server host name.
   - Specify a drive and folder as the installation destination. JP1/AO will be installed in the specified path on both the active and standby servers. If you see a message indicating that a restart is required after installation, restart the standby server.

   If the OS is Linux, you do not need to specify the installation destination. JP1/AO will be installed at a fixed path on the local disk.

Related topics

- 5.2 Installation prerequisites (for cluster systems)

5.3.4 Procedure for setting up the active server

Set up the active server.

To set up the active server:

1. If the ownership of the resource group has been moved to the standby server, use the cluster software to move the ownership back to the active server.
2. Use the cluster software to bring the resource group online.
3. On the active server, create a cluster settings file (*Common-Component-installation-folder*\conf\cluster.conf or /opt/HiCommand/Base64/conf/cluster.conf).

   For details, see 5.5 Cluster settings file (cluster.conf).
4. If the OS is Linux, on the active server, execute the `hcmds64srv` command with the `status` option specified to check the status of each service. If the database for the Common Component (HiRDB service) is not running, start the database by executing the `hcmds64dbsrv` command with the `start` option specified.
5. If the HAutomation Engine Web Service is running on the active server, stop the service by executing the `hcmds64srv` command with the `stop` and `server AutomationWebService` options specified.
6. On the active server, execute the `setupcluster` command.

Related topics

- 5.5 Cluster settings file (cluster.conf)
- JP1/AO services in the JP1/AO Administration Guide

5.3.5 Procedure for setting up the standby server

Set up the standby server.

To set up the standby server:

1. Use the cluster software to move the ownership of the resource group to the standby server.
2. On the standby server, create a cluster settings file (*Common-Component-installation-folder*\conf\cluster.conf or /opt/HiCommand/Base64/conf/cluster.conf).
3. If the OS is Linux, on the standby server, execute the `hcmds64srv` command with the `status` option specified to check the status of each service. If the database for Common Component (HiRDB service) is not running, start the database by executing the `hcmds64dbsrv` command with the `start` option specified.
4. If the HAutomation Engine Web Service is running on the standby server, stop the service by executing the `hcmds64srv` command with the `stop` and `server AutomationWebService` options specified.
5. On the standby server, execute the `setupcluster` command.

Related topics

- 5.5 Cluster settings file (cluster.conf)
- JP1/AO services in the JP1/AO Administration Guide

5.3.6 Procedure for using the cluster software to register services (in Windows)

If the OS is Windows, use the cluster software to register services.

To register services by using the cluster software:

1. Move **Current Owner** to the active server by using the cluster software.
2. Register services to the resource group by using the cluster software.

   Set the service dependencies in the order listed below. In the case of HiRDB/ClusterService _HD1, set the dependency to the shared disk and client access point.

   a. HiRDB/ClusterService _HD1

   b. HBase 64 Storage Mgmt SSO Service

   c. HBase 64 Storage Mgmt Web Service

   d. HBase 64 Storage Mgmt Web SSO Service

   e. HAutomation Engine Web Service

   If values are specified in **Startup Parameters** in the **General** Tab, remove the values.
3. Bring the resource group online by using the cluster software.

Related topics

- 5.6 Folders created on the JP1/AO shared disk

5.3.7 Procedure for using the cluster software to register resources and to set up the resource group (in Linux)

Use the cluster software to register resources and specify the settings for starting the resource group, stopping the resource group, and monitoring resources.

For details about the registration and setup procedures, see the documentation for the cluster software.

To register resources and configure the resource group by using the cluster software:

1. Use the cluster software to move the ownership of the resource group to the active server.
2. Use the cluster software to bring the resource group offline.
3. Use the cluster software to register resources.
4. Specify the settings such as those for starting the resource group, stopping the resource group, and monitoring resources.

   When specifying these settings, apply the following resource dependency:

If the resource group is online, the resources listed below (*a* to *f*) must start in the order from *a* to *f*. If the resource group is offline, the resources must start in the order from *f* to *a*.

For details about the commands that are to be registered in the cluster software to start, stop, monitor, and kill resources, see 5.7 Cluster service control commands to be registered in the cluster software.

a. IP address and shared disk

b. Database for Common Component

c. HBase 64 Storage Mgmt SSO Service

d. HBase 64 Storage Mgmt Web SSO Service

e. HBase 64 Storage Mgmt Web Service

f. HAutomation Engine Web Service

5. Use the cluster software to bring the resource group online.

Related topics

- 5.6 Folders created on the JP1/AO shared disk

5.4 Installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)

To set up a cluster system, you must install JP1/AO on both the active server and standby server.

To install JP1/AO, perform the procedure described below.

Table 5-4: Procedure for installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)

Task		Required/ optional	Reference
1	Perform the tasks that must be completed in advance.	Required	5.4.1 Tasks required before installation of JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)
2	Configure services before installation (if Common Component is already installed).	Required	5.4.2 Procedure for configuring services before installation (if Common Component is already installed)
3	Install JP1/AO on the active and standby servers (if Common Component is already installed).	Required	5.4.3 Procedures for installing JP1/AO on the active server and standby server (if Common Component is already installed)
4	Set up the active server (if Common Component is already installed).	Required	5.4.4 Procedure for setting up the active server (if Common Component is already installed)
5	Set up the standby server (if Common Component is already installed).	Required	5.4.5 Procedure for setting up the standby server (if Common Component is already installed)
6	Register services by using the cluster software (if Common Component is already installed).	Required	5.4.6 Procedure to register services by using the cluster software (if Common Component is already installed)

Related topics

- 5.2 Installation prerequisites (for cluster systems)

5.4.1 Tasks required before installation of JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)

Before you install JP1/AO in a cluster system, you must perform the tasks listed below.

Before you begin

- Check the installation prerequisites (for cluster system).
- Log in to the JP1/AO server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

5.4.2 Procedure for configuring services before installation (if Common Component is already installed)

Before you install JP1/AO in a cluster system, you must configure services.

To configure services before installation:

1. Make sure that JP1/AO or any conflicting product is not installed on either the active or standby servers.
   If it is installed, uninstall JP1/AO or conflicting product.
2. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the active server.
3. Use the cluster software to bring the above resource group online.
4. Use the cluster software to bring the Hitachi Command Suite services other than HiRDB/ClusterService _HD1 offline.
5. On the active server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
6. Use the cluster software to bring the HiRDB/ClusterService _HD1 service offline.
7. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the standby server.
8. Use the cluster software to bring the above resource group online.
9. Use the cluster software to bring the Hitachi Command Suite services other than HiRDB/ClusterService _HD1 offline.
10. On the standby server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
11. Use the cluster software to bring the HiRDB/ClusterService _HD1 service offline.
12. In the cluster software, suppress failover for the resource group where the Hitachi Command Suite products are registered.
    Right-click a service in the cluster software, and then select **Properties** and then **Policies**. Then specify the settings so that a restart does not occur if the resource fails. Perform this action for all services registered in the resource group in order to suppress failover.

Related topics

- 5.2 Installation prerequisites (for cluster systems)
- JP1/AO services in the JP1/Automatic Operation Administration Guide

5.4.3 Procedures for installing JP1/AO on the active server and standby server (if Common Component is already installed)

Install JP1/AO on the active server and standby server.

To install JP1/AO on the active server and standby server:

1. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the active server.

2. Install JP1/AO on the active server.
   - Specify a path on a shared disk for the location of the database.
   - Specify the logical host name for the JP1/AO server host name.
   - For the JP1/AO installation destination, specify the same drive and folder names in the active server and standby server.

   After installation, if a message is displayed indicating that a restart is required, restart the active server.
3. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the standby server.
4. Install JP1/AO on the standby server.
   - Specify a path on a shared disk for the location of the database.
   - Specify the logical host name for the JP1/AO server host name.
   - For the JP1/AO installation destination, specify the same drive and folder names in the active server and standby server.

   After installation, if a message is displayed indicating that a restart is required, restart the active server.

5.4.4 Procedure for setting up the active server (if Common Component is already installed)

Set up the active server.

To set up the active server:

1. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the active server.
2. If the HAutomation Engine Web Service is running on the active server, stop it by executing the `hcmds64srv` command with the `/stop /server AutomationWebService` option specified.
3. Execute the `setupcluster` command on the active server.

Related topics

- JP1/AO services in the JP1/Automatic Operation Administration Guide

5.4.5 Procedure for setting up the standby server (if Common Component is already installed)

Set up the standby server.

To set up the standby server:

1. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the standby server.
2. If the HAutomation Engine Web Service is running on the standby server, stop it by executing the `hcmds64srv` command with the `/stop /server AutomationWebService` option specified.

3. Execute the `setupcluster` command on the standby server.

Related topics

- JP1/AO services in the JP1/Automatic Operation Administration Guide

5.4.6 Procedure to register services by using the cluster software (if Common Component is already installed)

Register services by using the cluster software.

To register services by using the cluster software:

1. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the active server.
2. Use the cluster software to register services in the resource group where the Hitachi Command Suite products are registered.

   Set the service dependencies in the order listed below. In the case of HiRDB/ClusterService _HD1, set the dependency to the shared disk and client access point.

   a. HiRDB/ClusterService _HD1

   b. HBase 64 Storage Mgmt SSO Service

   c. HBase 64 Storage Mgmt Web Service

   d. HBase 64 Storage Mgmt Web SSO Service

   e. HAutomation Engine Web Service

   If values are specified in **Startup Parameters** in the **General** Tab, remove the values.
3. In the cluster software, enable failover for the resource group where the Hitachi Command Suite products are registered.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if the resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.
4. Bring the resource group online by using the cluster software.

Related topics

- 5.6 Folders created on the JP1/AO shared disk
- 5.5 Cluster settings file (cluster.conf)

5.5 Cluster settings file (cluster.conf)

This is the definition file created on both the active server and the standby server and used for configuring a cluster.

Create the cluster settings file according to the procedures for setting up the cluster and changing the host name.

Format

specification-key-name=setting

Installation folder

Common-Component-installation-folder\conf or /opt/HiCommand/Base64/conf

Description

One specification key and setting can be specified per line.

Active server settings

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

Standby server settings

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

Related topics

- 5.2 Installation prerequisites (for cluster systems)
- 5.3 Installing JP1/AO in a cluster system
- 5.4 Installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)

5.6 Folders created on the JP1/AO shared disk

When JP1/AO is installed on a cluster system, executing the `setupcluster` command creates the following folders on the shared disk that is specified when the command is executed.

Table 5-5: Folders created on the shared disk (in Windows)

Product	Application	Created folder
JP1/AO	Folder for definition files	*shared-folder-name*\jp1ao\conf
	Service template folder	*shared-folder-name*\jp1ao\contents
	Log file output folder	*shared-folder-name*\jp1ao\logs
	Folder for system files	*shared-folder-name*\jp1ao\system
	Work folder	*shared-folder-name*\jp1ao\work
	Data folder	*shared-folder-name*\jp1ao\data
	Folder for development service templates (plug-ins) and service template packages	*shared-folder-name*\jp1ao\develop
Common Component	Database installation folder	*shared-folder-name*\Base64\database#
	Folder for setting up the active server	*shared-folder-name*\Base64\online#
	Folder for setting up the standby server	*shared-folder-name*\Base64\standby#

#

If Common Component already exits in the cluster environment, a new folder is not created on the shared disk.

Table 5-6: Folders created on the shared disk (in Linux)

Product	Application	Created folder
JP1/AO	Folder for definition files	*shared-folder-name*/jp1ao/conf
	Service template folder	*shared-folder-name*/jp1ao/contents
	Log file output folder	*shared-folder-name*/jp1ao/logs
	Folder for system files	*shared-folder-name*/jp1ao/system
	Work folder	*shared-folder-name*/jp1ao/work
	Data folder	*shared-folder-name*/jp1ao/data
	Folder for development service templates (plug-ins) and service template packages	*shared-folder-name*/jp1ao/develop
Common Component	Database installation folder	*shared-folder-name*/Base64/database
	Folder for setting up the active server	*shared-folder-name*/Base64/online
	Folder for setting up the standby server	*shared-folder-name*/Base64/standby

Related topics

- 5.3 Installing JP1/AO in a cluster system
- 5.4 Installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration)

5.7 Cluster service control commands to be registered in the cluster software

If you build a cluster configuration in Linux, by registering the commands that control the JP1/AO-related resources in the cluster software, you can specify the settings for starting, stopping, monitoring, and killing resources. In JP1/AO, these commands are called *cluster service control commands*.

This section describes the tasks required before the cluster service control commands can be registered in the cluster software. This section also describes the cluster service control commands in detail.

For details about the procedure for registering the cluster service control commands in the cluster software, see the documentation for the cluster software.

5.7.1 Tasks required before the cluster service control commands can be registered

This subsection describes the tasks required before cluster service control commands can be registered in the cluster software.

Renaming model files to create the cluster service control commands

1. Copy the model files for the cluster service control commands in a directory. These model files have the file name extension .model, and are stored in the /opt/jp1ao/tools directory.

   The following are the model files to be copied:

   - sc_automation.model
   - sc_hbase64_web.model
   - sc_hbase64_hweb.model
   - sc_hbase64_hsso.model
   - sc_hbase64_hirdb.model
2. Rename the copied model files by deleting their file name extension (.model).

Editing the cluster service control commands

1. Specify the Common Component installation directory for the following shell variable of each cluster service control command:

   `HCMDS_HOME=`*`common-component-installation-directory`*
2. Specify the logical host name for the following shell variable of the sc_hbase64_hirdb cluster service control command. Note that the logical host name you specify for the shell variable is the value of the virtualhost key in the cluster.conf file.

   `PDHOST=`*`logical-host-name`*

> **Important**
>
> When you update the version of JP1/AO, the model files for the cluster service control commands might be updated. Therefore, after you perform an upgrade installation of JP1/AO, check whether the version of the created cluster service control commands and the version of the model files are the same. If the version

of model files has been updated, copy those files and edit them as cluster service control commands. The version is specified as a comment in the files.

5.7.2 Command that controls the database for Common Component (sc_hbase64_hirdb)

This subsection provides information required to register (in the cluster software) the `sc_hbase64_hirdb` command, which is used to control the database for Common Component.

Command to be used:

`sc_hbase64_hirdb`

Location of the command:

/opt/jp1ao/tools

Table 5-7: Information required to register the sc_hbase64_hirdb command

Registerable mode	Description
Start	Use this mode to start the database for Common Component. Format: `sc_hbase64_hirdb start` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Start mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Stop	Use this mode to stop the database for Common Component. Format: `sc_hbase64_hirdb stop` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Stop mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Monitor	Use this mode to check whether the database for Common Component is operating normally. You need to register this mode only if you want a failover to occur when the database fails. Format: `sc_hbase64_hirdb status` Result judgment: Return code 0 (normal) The database for Common Component is operating normally. Return code 3 (not running) The process of the database for Common Component is stopped due to a problem. If this return code is returned, assume that an error has occurred.

5.7.3 Command that controls the HBase 64 Storage Mgmt SSO Service (sc_hbase64_hsso command)

This subsection provides information required to register (in the cluster software) the `sc_hbase64_hsso` command, which is used to control the HBase 64 Storage Mgmt SSO Service.

Command to be used:

```
sc_hbase64_hsso
```

Location of the command:

/opt/jp1ao/tools

Table 5-8: Information required to register the sc_hbase64_hsso command

Registerable mode	Description
Start	Use this mode to start the HBase 64 Storage Mgmt SSO Service. Format: `sc_hbase64_hsso start` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Start mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Stop	Use this mode to stop the HBase 64 Storage Mgmt SSO Service. Format: `sc_hbase64_hsso stop` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Stop mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Monitor	Use this mode to check whether the HBase 64 Storage Mgmt SSO Service is operating normally. You need to register this mode only if you want a failover to occur when the service fails. Format: `sc_hbase64_hsso status` Result judgment: Return code 0 (normal) The HBase 64 Storage Mgmt SSO Service is operating normally. Return code 3 (not running) The process of the HBase 64 Storage Mgmt SSO Service is stopped due to a problem. If this return code is returned, assume that an error has occurred.

5.7.4 Command that controls the HBase 64 Storage Mgmt Web SSO Service (sc_hbase64_hweb)

This subsection provides information required to register (in the cluster software) the `sc_hbase64_hweb` command, which is used to control the HBase 64 Storage Mgmt Web SSO Service.

Command to be used:

```
sc_hbase64_hweb
```

Location of the command:

/opt/jp1ao/tools

Table 5-9: Information required to register the sc_hbase64_hweb command

Registerable mode	Description
Start	Use this mode to start the HBase 64 Storage Mgmt Web SSO Service.

Registerable mode	Description
Start	Format: `sc_hbase64_hweb start` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Start mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Stop	Use this mode to stop the HBase 64 Storage Mgmt Web SSO Service. Format: `sc_hbase64_hweb stop` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Stop mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Monitor	Use this mode to check whether the HBase 64 Storage Mgmt Web SSO Service is operating normally. You need to register this mode only if you want a failover to occur when the service fails. Format: `sc_hbase64_hweb status` Result judgment: Return code 0 (normal) The HBase 64 Storage Mgmt Web SSO Service is operating normally. Return code 3 (not running) The process of the HBase 64 Storage Mgmt Web SSO Service is stopped due to a problem. If this return code is returned, assume that an error has occurred.

5.7.5 Command that controls the HBase 64 Storage Mgmt Web Service (sc_hbase64_web)

This subsection provides information required to register (in the cluster software) the `sc_hbase64_web` command, which is used to control the HBase 64 Storage Mgmt Web Service.

Command to be used:

`sc_hbase64_web`

Location of the command:

/opt/jp1ao/tools

Table 5-10: Information required to register the sc_hbase64_web command

Registerable mode	Description
Start	Use this mode to start the HBase 64 Storage Mgmt Web Service. Format: `sc_hbase64_web start` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Start mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Stop	Use this mode to stop the HBase 64 Storage Mgmt Web Service. Format: `sc_hbase64_web stop`

Registerable mode	Description
Stop	Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Stop mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Monitor	Use this mode to check whether the HBase 64 Storage Mgmt Web Service is operating normally. You need to register this mode only if you want a failover to occur when the service fails. Format: `sc_hbase64_web status` Result judgment: Return code 0 (normal) The HBase 64 Storage Mgmt Web Service is operating normally. Return code 3 (not running) The process of the HBase 64 Storage Mgmt Web Service is stopped due to a problem. If this return code is returned, assume that an error has occurred.

5.7.6 Command that controls the HAutomation Engine Web Service (sc_automation)

This subsection provides information required to register (in the cluster software) the `sc_automation` command, which is used to control the HAutomation Engine Web Service.

Command to be used:

`sc_automation`

Location of the command:

/opt/jp1ao/tools

Table 5-11: Information required to register the sc_automation command

Registerable mode	Description
Start	Use this mode to start the HAutomation Engine Web Service. Format: `sc_automation start` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Start mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Stop	Use this mode to stop the HAutomation Engine Web Service. Format: `sc_automation stop` Result judgment: Judge the result from the result of the command executed in Monitor mode. Because the command in Stop mode returns 0 as normal termination or 1 as an argument error, you cannot judge the result from the return code.
Monitor	Use this mode to check whether the HAutomation Engine Web Service is operating normally. You need to register this mode only if you want a failover to occur when the service fails. Format: `sc_automation status`

Registerable mode	Description
Monitor	Result judgment: Return code 0 (normal) The HAutomation Engine Web Service is operating normally. Return code 3 (not running) The process of the HAutomation Engine Web Service is stopped due to a problem. If this return code is returned, assume that an error has occurred.

6 Overwrite or upgrade installation

This chapter explains how to perform an overwrite or upgrade installation of JP1/AO.

6.1 Overwrite or upgrade installation procedure

The overwrite or upgrade installation procedure consists of the following steps.

Table 6-1: Overwrite or upgrade installation procedure

Task		Required/ optional	Reference
1	(If the OS is Windows) To upgrade the JP1/AO version from 10 to 12, perform the pre-installation tasks.	Required	6.2.1 Tasks required before an upgrade installation (when upgrading from version 10 to 12)
2	If the JP1/AO server OS is Linux 8, verify that the ports that JP1/AO will use are not in use.	Required	1.2.3 Check the port to use
3	Perform an overwrite or upgrade installation of JP1/AO.	Required	For non-cluster systems: 6.3 Procedure to perform an overwrite or upgrade installation of JP1/AO (non-cluster system) For cluster systems: 6.5 Procedure to perform an overwrite or upgrade installation of JP1/AO (for a Windows cluster system) 6.6 Procedure to perform an overwrite or upgrade installation of JP1/AO (for a Linux cluster system)
4	If you do not use JP1/Base after upgrading JP1/AO from a version earlier than 11-10 to 11-10 or later, uninstall JP1/Base.	Optional	*Installation and Setup* in the *JP1/Base User's Guide*
5	Perform an overwrite installation of JP1/AO Content Pack.	Optional	6.7 Procedure to perform an overwrite installation of JP1/AO Content Pack
6	(If the OS is Windows) To upgrade the JP1/AO version from 10 to 12, perform the post-installation tasks.	Required	6.4.1 Tasks required after an upgrade installation (when upgrading from version 10 to 12)
7	In Windows, if the following case applies, re-create the startup-order definition file of JP1/Base. In an environment where JP1/AO does not coexist with JP1/AJS3, JP1/Base Control Service is used to start JP1/AJS services after upgrading JP1/AO from a version earlier than 11-10 to 11-10 or later.	Optional	6.4.2 Tasks required after an upgrade installation (when automatic startup for JP1/AJS3 is enabled) *Setting the service start and stop sequences* in the *JP1/Base User's Guide*
8	In an environment where JP1/AO coexists with JP1/AJS3, if JP1/AO is upgraded from a version earlier than 11-10, perform the following tasks: • Delete the JP1/AJS3 scheduler service and embedded database. • Change and delete the execution agents of JP1/AJS3. • Uninstall JP1/AJS3 - Manager.	Required	6.4.3 Tasks required after an upgrade installation (in an environment in which JP1/AO coexists with JP1/AJS3) A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

6.2 Tasks required before an overwrite or upgrade installation

6.2.1 Tasks required before an upgrade installation (when upgrading from version 10 to 12)

This section describes the tasks that you must perform before upgrading the version of JP1/AO from 10 to 12 in Windows.

Important

If you upgrade JP1/AO from version 10-02 or earlier, do not uninstall JP1/AJS3 - View when there are service templates that were created in a JP1/AO environment of version 10-02 or earlier. JP1/AJS3 - View might be used when migrating service templates to Service Builder.

Before you begin

- Back up the environment in case of a failure occurring during the upgrade installation. If you upgrade the version of JP1/AO from 10 to 12, you will no longer be able to restore the data that was used in version 10. If an upgrade installation fails, install JP1/AO version 10 or earlier as a new installation, and then restore the data from a backup.
- If the port number used in JP1/AO version 10 or earlier has been changed from the default port number, record the current port number. If you upgrade the version to 12, the port number is reset to the default port number (22015). After the upgrade installation finishes, change the default port number to the port number that you recorded.
- If the default port number (23015) for JP1/AO version 10 or earlier will no longer be used as the port number of JP1/AO, you must delete the port number from the firewall exceptions list. In version 12 or later, if you change the port number from the default port number (22015), you must review the firewall settings.
- If HTTPS connections are enabled, manually back up the private key file and SSL server certificate file. After the version has been upgraded, specify the HTTPS connection settings again.

6.2.2 Check the port to use

Before you install JP1/AO on Linux 8, verify that the ports that JP1/AO will use on the JP1/AO server are not in use by other products. If a port is being used by another product, neither product might operate correctly.

To ensure that the necessary ports are not in use, use the `netstat` or `ss` command.

You must verify that port numbers 22170 - 22173 are not used by other products because this causes a new, overwrite, or upgrade installation to fail.

6.3 Procedure to perform an overwrite or upgrade installation of JP1/AO (non-cluster system)

Use the Hitachi Integrated Installer or Hitachi Program Product Installer to overwrite-install or upgrade-install JP1/AO. If you choose to use the Hitachi Program Product Installer, for details about how to use it, see 1.3.2 Installation procedure using the Hitachi Program Product Installer.

Before you begin

Log in to the JP1/AO server as a user with administrator or root permissions on the OS.

Note that the following files and folders are not overwritten during the overwrite or upgrade installation:

JP1/AO-installation-folder`\conf` or `/opt/jp1ao/conf`

- config_user.properties
- command_user.properties
- mailDefinition_ja.conf
- mailDefinition_en.conf
- mailDefinition_zh.conf

JP1/AO-installation-folder`\conf\plugin` or `/opt/jp1ao/conf/plugin`

- charsetMapping_user.properties
- krb5.conf (in Windows)
- login.conf (in Windows)
- Files in the destinations folder

JP1/AO-installation-folder`\docroot\help\ja` or `/opt/jp1ao/docroot/help/ja`

- INDEX.HTM

JP1/AO-installation-folder`\docroot\help\en` or `/opt/jp1ao/docroot/help/en`

- INDEX.HTM

JP1/AO-installation-folder`\docroot\help\zh` or `/opt/jp1ao/docroot/help/zh`

- INDEX.HTM

Common-Component-installation-folder`\uCPSB\CC\web\containers\AutomationWebService\webapps\Automation\services\custom` (in Windows), `/opt/HiCommand/Base64/uCPSB/CC/web/containers/AutomationWebService/webapps/Automation/services/custom` (in Linux 6, Linux 7, SUSE Linux 12), or `/opt/jp1ao/webapps/webroot/Automation/Automation/services/custom` (in Linux 8)

- All files in the above folder

To perform an overwrite or upgrade installation:

1. Insert the distribution medium into the drive.
2. Continue the configuration process as prompted by the wizard.[#]

   In case of a failure during overwrite or upgrade installation, you can back up the database that is shared with the Hitachi Command Suite products, and can set the folder in which the database is to be backed up. You must specify these settings only if Hitachi Command Suite products have already been installed.

3. Check the summary that is displayed to verify the settings that you have entered in the wizard thus far.#
4. Start the installation of JP1/AO.
5. After the installation is complete, start the JP1/AO services by executing the `hcmds64srv` command with the `start` option specified.
6. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO - Contents service templates or Service Template Set into JP1/AO.
7. If necessary, apply updates to the components used in the service template and changes to the service template to the service.

#

If the Hitachi Program Product Installer is used, the installation wizard is not displayed during installation.

Related topics

- 1.2 Pre-installation tasks
- Updating the components used in a service template in the JP1/AO Administration Guide
- Applying service template changes to services in the JP1/AO Administration Guide

6.4 Tasks required after an upgrade installation

6.4.1 Tasks required after an upgrade installation (when upgrading from version 10 to 12)

This section describes the tasks that you must perform after upgrading the version of JP1/AO from 10 to 12 in Windows.

- When you have just upgraded the version, back up the environment. If you upgrade the version of JP1/AO from 10 to 12, you will no longer be able to restore the data that was used in version 10. If a problem occurs during operation, restore the data that you backed up immediately after the upgrade installation.
- When the upgrade installation finishes, the port number is reset to the default port number. If you do not want to use the default port number, manually set the desired port number.
- In a cluster environment, after upgrade installation finishes, make sure that the same port number is set in the following definition files. Note that the setting locations differ depending on the communication protocol used for communication between JP1/AO and the Web browser.

  For HTTP protocol:

  - The user_httpsd.conf file in *Common-Component-installation-folder*\uCPSB\httpsd\conf

    ```
    Listen port-number
    Listen [::]:port-number
    ```

  - The command property file (command_user.properties) in *shared-folder-name*\jp1ao\conf

  For HTTPS protocol:

  - The user_httpsd.conf file in *Common-Component-installation-folder*\uCPSB\httpsd\conf

    ```
    Listen 127.0.0.1:port-number
    ```

  - The command property file (command_user.properties) in *shared-folder-name*\jp1ao\conf
- In JP1/AO version 12, because the names of installation folders and Common Component commands have been changed, review their settings.

Related topics

- 2.3 Command property file (command_user.properties)
- 4.5 Procedure to change the port number

6.4.2 Tasks required after an upgrade installation (when automatic startup for JP1/AJS3 is enabled)

In a Windows environment in which JP1/AO does not coexist with JP1/AJS3, if JP1/AO is upgraded from a version earlier than 11-10 to 11-10 or later, and if JP1/Base Control Service is used to start JP1/AJS3 services, re-create the startup-order definition file (*JP1SVPRM.DAT*) by using the `cpysvprm` command.

For details about the startup-order definition file, see the topic Setting the service start and stop sequences in the *JP1/Base User's Guide*.

6.4.3 Tasks required after an upgrade installation (in an environment in which JP1/AO coexists with JP1/AJS3)

In an environment in which JP1/AO coexists with JP1/AJS3, perform the following tasks after upgrading JP1/AO to 11-10 or a later version:

- Delete the JP1/AJS3 scheduler service and embedded database.
- Change or delete execution agents.
  - Change the number of concurrently executable instances of the `@SYSTEM` execution agent.
  - Delete the `loop` and `userResponse` execution agents.
- Uninstall JP1/AJS3 - Manager
  If JP1/AJS3 - Manager is not being used, uninstall it.

Related topics

- 4.8 Procedure to change the maximum number of plug-ins that can be executed concurrently
- A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

6.5 Procedure to perform an overwrite or upgrade installation of JP1/AO (for a Windows cluster system)

In a cluster system, you must perform an overwrite or upgrade installation of JP1/AO on both the active and standby servers.

The overwrite or upgrade installation procedure consists of the following steps.

Table 6-2: Overwrite or upgrade installation procedure (for a Windows cluster system)

Task		Required/ optional	Reference
1	Perform the tasks that must be completed in advance.	Required	6.5.1 Tasks that must be completed before an overwrite or upgrade installation (Windows) Perform the following operation if you upgrade JP1/AO from version 10 to 12. 6.2.1 Tasks required before an upgrade installation (when upgrading from version 10 to 12)
2	Configure the services before starting overwrite or upgrade installation.	Required	6.5.2 Procedure to configure services before overwrite or upgrade installation (Windows)
3	Perform an overwrite or upgrade installation of JP1/AO on the active server.	Required	6.5.3 Procedure to perform an overwrite or upgrade installation of JP1/AO on the active server(Windows)
4	Perform an overwrite or upgrade installation of JP1/AO on the standby server.	Required	6.5.4 Procedure to perform an overwrite or upgrade installation of JP1/AO on the standby server (Windows)
5	If you perform an upgrade installation from a cluster environment built with a JP1/AO version earlier than 11-10, register the services.	Required	5.3.6 Procedure for using the cluster software to register services (in Windows)
6	Enable failover of the resource group.	Required	6.5.5 Procedure for enabling failover of the resource group (Windows)
7	If you do not use JP1/Base after upgrading JP1/AO from a version earlier than 11-10 to 11-10 or later, uninstall JP1/Base.	Optional	*Installation and Setup* in the *JP1/Base User's Guide*
8	If you upgrade the version of JP1/AO from 10 to 12, perform post-upgrade tasks.	Required	6.4.1 Tasks required after an upgrade installation (when upgrading from version 10 to 12)
9	If the following case applies, re-create the startup-order definition file of JP1/Base. In an environment where JP1/AO does not coexist with JP1/AJS3, JP1/Base Control Service is used to start JP1/AJS services after upgrading JP1/AO from a version earlier than 11-10 to 11-10 or later.	Optional	6.4.2 Tasks required after an upgrade installation (when automatic startup for JP1/AJS3 is enabled) *Setting the service start and stop sequences* in the *JP1/Base User's Guide*
10	In an environment where JP1/AO coexists with JP1/AJS3, if JP1/AO is upgraded from a version earlier than 11-10, perform the following tasks:	Required	6.4.3 Tasks required after an upgrade installation (in an environment in which JP1/AO coexists with JP1/AJS3) A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

Task		Required/ optional	Reference
10	• Delete the JP1/AJS3 scheduler service and embedded database. • Change and delete the execution agents of JP1/AJS3. • Uninstall JP1/AJS3 - Manager.	Required	6.4.3 Tasks required after an upgrade installation (in an environment in which JP1/AO coexists with JP1/AJS3) A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

Related topics

- 5.2 Installation prerequisites (for cluster systems)

6.5.1 Tasks that must be completed before an overwrite or upgrade installation (Windows)

Before you perform an overwrite or upgrade installation of JP1/AO, you must perform the tasks listed below.

Before you begin

Log in to the JP1/AO server as a user with not only administrator permissions on the OS, but also administrator permissions on the cluster.

Note that the following files are not overwritten during the overwrite or upgrade installation:

shared-folder-name\conf

- config_user.properties
- command_user.properties
- mailDefinition_ja.conf
- mailDefinition_en.conf
- mailDefinition_zh.conf

shared-folder-name\conf\plugin

- charsetMapping_user.properties
- krb5.conf
- login.conf
- Files in the `destinations` folder

JP1/AO-installation-folder\docroot\help\ja

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\en

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\zh

- INDEX.HTM

/opt/jp1ao/tools

- Cluster service control commands that you created

Common-Component-installation-folder\uCPSB\CC\web\containers\AutomationWebService\webapps\Automation\services\custom

- All files in the above folder

6.5.2 Procedure to configure services before overwrite or upgrade installation (Windows)

You must configure services before installation.

To configure services before installation:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
3. Use the cluster software to bring the above resource group online.
4. Use the cluster software to bring the services and scripts offline.

   If the Hitachi Command Suite products are installed, bring all services and scripts offline except for the following services:

   - HiRDB/ClusterService _HD0 (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HiRDB/ClusterService _HD1 (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - JP1/Base_*logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
   - JP1/Base Event _*logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)

   If the Hitachi Command Suite products are not installed, bring the following services and script offline:

   - HAutomation Engine Web Service
   - HAutomation Engine *logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
   - HBase Storage Mgmt Common Service (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HBase Storage Mgmt Web Service (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HBase 64 Storage Mgmt SSO Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - HBase 64 Storage Mgmt Web Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - HBase 64 Storage Mgmt Web SSO Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - `stopcluster` command[#](for an upgrade installation in a cluster environment built with a JP1/AO version 10)

5. On the active server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
6. Use the cluster software to bring the following services offline:
   - HiRDB/ClusterService _HD0 (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HiRDB/ClusterService _HD1 (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - JP1/Base_*logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
   - JP1/Base Event _*logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
7. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
8. Use the cluster software to bring the above resource group offline.
9. Use the cluster software to bring the services and scripts offline.
   If the Hitachi Command Suite products are installed, bring the services and scripts offline, except for the following services:
   - HiRDB/ClusterService _HD0 (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HiRDB/ClusterService _HD1 (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - JP1/Base_*logical-host-name*
     (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
   - JP1/Base Event _*logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)

   If the Hitachi Command Suite products are not installed, bring the following services and script offline:
   - HAutomation Engine Web Service
   - HAutomation Engine *logical-host-name* (for an upgrade installation in a cluster environment built with a version of JP1/AO earlier than 11-10)
   - HBase Storage Mgmt Common Service (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HBase Storage Mgmt Web Service (for an upgrade installation in a cluster environment built with JP1/AO version 10)
   - HBase 64 Storage Mgmt SSO Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - HBase 64 Storage Mgmt Web Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - HBase 64 Storage Mgmt Web SSO Service (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
   - `stopcluster` command[#]
     (for an upgrade installation in a cluster environment built with JP1/AO version 10)
10. On the standby server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
11. Use the cluster software to bring the following services offline:

- HiRDB/ClusterService _HD0 (for an upgrade installation in a cluster environment built with JP1/AO version 10)
- HiRDB/ClusterService _HD1 (for an overwrite or upgrade installation in a cluster environment built with JP1/AO version 11 or later)
- JP1/Base_*logical-host-name*
  (for an upgrade installation in a cluster environment built with JP1/AO version 10)
- JP1/Base Event _*logical-host-name* (for an upgrade installation in a cluster environment built with JP1/AO version 10)

12. In the cluster software, suppress failover for the resource group where JP1/AO is registered.
    Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart does not occur if the resource fails. Perform this action for all services and scripts registered in the resource group in order to suppress failover.

#
This command does not exist when an upgrade installation is performed in a cluster environment built with JP1/AO whose version is 10-12-01 or earlier or 10-13 (except version 10-13-01 or later) .

Related topics

- JP1/AO services in the JP1/Automatic Operation Administration Guide

6.5.3 Procedure to perform an overwrite or upgrade installation of JP1/AO on the active server(Windows)

This subsection describes how to overwrite-install or upgrade-install JP1/AO on the active server in Windows.

To perform an overwrite or upgrade installation of JP1/AO on the active server:

1. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
2. (If the upgrade installation target is a cluster environment built with JP1/AO version 10) Unregister the following services from the cluster software:
   - HiRDB/ClusterService _HD0
   - HAutomation Engine Web Service
   - HAutomation Engine *logical-host-name*
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - `stopcluster` command
3. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, if the service (JP1/Base_*logical-host-name*) is online on the active server, bring it offline.
4. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, Start the service (JP1/Base) on the active server.
5. Perform an overwrite or upgrade installation of JP1/AO on the active server.
6. (If the upgrade installation target is a cluster environment built with JP1/AO version 10) On the active server, create a cluster settings file (*Common-Component-installation-folder*¥conf¥cluster.conf).

For details, see 5.5 Cluster settings file (cluster.conf).

7. If the HAutomation Engine Web Service is running on the active server, stop the service by executing the `hcmds64srv` command with the `/stop /server AutomationWebService` option specified.
8. Execute the `setupcluster` command on the active server.

6.5.4 Procedure to perform an overwrite or upgrade installation of JP1/AO on the standby server (Windows)

This subsection describes how to overwrite-install or upgrade-install JP1/AO on the standby server in Windows.

To perform an overwrite or upgrade installation of JP1/AO on the standby server:

1. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
2. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, if the service (JP1/Base_*logical-host-name*) is online on the standby server, bring it offline.
3. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, Start the service (JP1/Base) on the standby server.
4. Perform an overwrite or upgrade installation of JP1/AO on the standby server.
5. (If the upgrade installation target is a cluster environment built with JP1/AO version 10) On the standby server, create a cluster settings file (*Common-Component-installation-folder*¥conf¥cluster.conf).

   For details, see 5.5 Cluster settings file (cluster.conf).
6. If the HAutomation Engine Web Service is running on the standby server, stop the service by executing the `hcmds64srv` command with the `/stop /server AutomationWebService` option specified.
7. Execute the `setupcluster` command on the standby server.

6.5.5 Procedure for enabling failover of the resource group (Windows)

This subsection describes how to enable failover of the resource group.

To enable failover of the resource group:

1. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
2. Use the cluster software to enable failover of the resource group where JP1/AO is registered.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if the resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.
3. Bring the resource group online by using the cluster software.
4. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO - Contents service templates or Service Template Set into JP1/AO.
5. If necessary, apply updates to the components used in the service template and changes to the service template to the service.

Related topics

- Updating the components used in a service template in the JP1/AO Administration Guide
- Applying service template changes to services in the JP1/AO Administration Guide

6.6 Procedure to perform an overwrite or upgrade installation of JP1/AO (for a Linux cluster system)

In a cluster system, you must perform an overwrite or upgrade installation of JP1/AO on both the active and standby servers.

The overwrite or upgrade installation procedure consists of the following steps.

Table 6-3: Overwrite or upgrade installation procedure (for a Linux cluster system)

Task		Required/ optional	Reference
1	Perform the tasks that must be completed in advance.	Required	6.6.1 Tasks that must be completed before an overwrite or upgrade installation (Linux)
2	Configure the services before starting overwrite or upgrade installation.	Required	6.6.2 Procedure to configure resources before overwrite or upgrade installation (Linux)
3	Perform an overwrite or upgrade installation of JP1/ AO on the active server.	Required	6.6.3 Procedure to perform an overwrite or upgrade installation of JP1/AO on the active server(Linux)
4	Perform an overwrite or upgrade installation of JP1/ AO on the standby server.	Required	6.6.4 Procedure to perform an overwrite or upgrade installation of JP1/AO on the standby server (Linux)
5	change the resource settings	Required	6.6.5 Procedure for changing resource settings (Linux)
6	If you perform an upgrade installation from a cluster environment built with a JP1/AO version earlier than 11-10, register the resources and to set up the resource group.	Required	5.3.7 Procedure for using the cluster software to register resources and to set up the resource group (in Linux)
7	If you do not use JP1/Base after upgrading JP1/AO from a version earlier than 11-10 to 11-10 or later, uninstall JP1/Base.	optional	*Installation and Setup* in the *JP1/Base User's Guide*
8	In an environment where JP1/AO coexists with JP1/AJS3, if JP1/AO is upgraded from a version earlier than 11-10, perform the following tasks: • Delete the JP1/AJS3 scheduler service and embedded database. • Change and delete the execution agents of JP1/AJS3. • Uninstall JP1/AJS3 - Manager.	Required	6.4.3 Tasks required after an upgrade installation (in an environment in which JP1/AO coexists with JP1/AJS3) A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

Related topics

- 5.2 Installation prerequisites (for cluster systems)

6.6.1 Tasks that must be completed before an overwrite or upgrade installation (Linux)

Before you perform an overwrite or upgrade installation of JP1/AO, you must perform the tasks listed below.

Before you begin

Log in to the JP1/AO server as a user with not only root permissions on the OS, but also administrator permissions on the cluster.

Note that the following files are not overwritten during the overwrite or upgrade installation:

shared-folder-name`/jp1ao/conf`

- config_user.properties
- command_user.properties
- mailDefinition_ja.conf
- mailDefinition_en.conf
- mailDefinition_zh.conf

shared-folder-name`/jp1ao/conf/plugin`

- charsetMapping_user.properties
- Files in the `destinations` folder

JP1/AO-installation-folder`/opt/jp1ao/docroot/help/ja`

- INDEX.HTM

JP1/AO-installation-folder`/opt/jp1ao/docroot/help/en`

- INDEX.HTM

JP1/AO-installation-folder`/opt/jp1ao/docroot/help/zh`

- INDEX.HTM

`/opt/jp1ao/tools`

- Cluster service control commands that you created

`/opt/HiCommand/Base64/uCPSB/CC/web/containers/AutomationWebService/webapps/Automation/services/custom` (in Linux 6, Linux 7, SUSE Linux 12) or `/opt/jp1ao/webapps/webroot/Automation/Automation/services/custom` (in Linux 8)

- All files in the above folder

6.6.2 Procedure to configure resources before overwrite or upgrade installation (Linux)

You must configure resources before installation.

To configure resources before installation:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Use the cluster software to disable starting, stopping, and monitoring resources other than the following resources:
   - Shared disk
   - Logical host name

- Logical IP address

3. Use the cluster software to bring the resource group online.

6.6.3 Procedure to perform an overwrite or upgrade installation of JP1/AO on the active server(Linux)

This subsection describes how to overwrite-install or upgrade-install JP1/AO on the active server in Linux.

To perform an overwrite or upgrade installation of JP1/AO on the active server:

1. Use the cluster software to move the resource group that includes JP1/AO to the active server.
2. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, if the JP1/Base logical host is running on the active server, stop the logical host.
3. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, on the active server, start the JP1/Base physical host.
4. On the active server, overwrite-install or upgrade-install JP1/AO.
5. On the active server, execute the `hcmds64srv` command with the `status` option specified to check the status of each service. If the database for Common Component (HiRDB service) is not running, start the database by executing the `hcmds64dbsrv` command with the `start` option specified.
6. If the HAutomation Engine Web Service is running on the active server, stop the service by executing the `hcmds64srv` command with the `-stop -server AutomationWebService` option specified.
7. On the active server, execute the `setupcluster` command.

6.6.4 Procedure to perform an overwrite or upgrade installation of JP1/AO on the standby server (Linux)

This subsection describes how to overwrite-install or upgrade-install JP1/AO on the standby server in Linux.

To perform an overwrite or upgrade installation of JP1/AO on the standby server:

1. Use the cluster software to move the resource group that includes JP1/AO to the standby server.
2. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, if the JP1/Base logical host is running on the standby server, stop the logical host.
3. When the upgrade installation target is a cluster environment built with a JP1/AO version earlier than 11-10, on the standby server, start the JP1/Base physical host.
4. On the standby server, overwrite-install or upgrade-install JP1/AO.
5. On the standby server, execute the `hcmds64srv` command with the `status` option specified to check the status of each service. If the database for Common Component (HiRDB service) is not running, start the database by executing the `hcmds64dbsrv` command with the `start` option specified.
6. If the HAutomation Engine Web Service is running on the standby server, stop the service by executing the `hcmds64srv` command with the `-stop -server AutomationWebService` option specified.
7. On the active server, execute the `setupcluster` command.

6.6.5 Procedure for changing resource settings (Linux)

This subsection describes how to change the settings for starting, stopping, and monitoring resources.

To change resource settings:

1. Use the cluster software to move resource groups that are registered in JP1/AO to the active server.
2. If JP1/AO is upgraded from a version earlier than 11-10, check whether the version of cluster service control commands and the version of model files are the same. If the model files have been upgraded, re-create the cluster service control commands.

   For the procedure for re-creating cluster service control commands, see 5.7.1 Tasks required before the cluster service control commands can be registered.
3. Use the cluster software to bring the resource group offline.
4. Use the cluster software to re-enable starting, stopping, and monitoring the resources other than the following resources:
   - Shared disk
   - Logical host name
   - Logical IP address

   If JP1/AO is upgraded from a version earlier than 11-10, review resources that have been registered in resource groups and set resource dependencies.

   For the procedure for setting resource dependencies, see 5.3.7 Procedure for using the cluster software to register resources and to set up the resource group (in Linux).
5. Use the cluster software to bring the resource group online.
6. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO - Contents service templates or Service Template Set into JP1/AO.
7. If necessary, apply updates to the components used in the service template and changes to the service template to the service.

Related topics

- Updating the components used in a service template in the JP1/AO Administration Guide
- Applying service template changes to services in the JP1/AO Administration Guide

6.7 Procedure to perform an overwrite installation of JP1/AO Content Pack

The following describes how to perform an overwrite installation of JP1/AO Content Pack. When an overwrite installation of JP1/AO Content Pack is performed, the previous version of Service Template Set is overwritten by the latest one.

Before you begin

- Log in as a user with administrator or root permissions.
- Confirm that JP1/AO is installed.

  Note that because JP1/AO Content Pack does not conflict with other products, you do not have to check for conflicting products.
- All the files and folders in the JP1/AO Content Pack installation folder are deleted during overwrite installation. Back up the necessary files and folders.

To perform an overwrite installation of JP1/AO Content Pack:

1. Insert the distribution medium into the drive.
2. Check the installation folder for JP1/AO Content Pack according to the wizard.#

   You cannot change the installation folder for JP1/AO Content Pack.
3. Click the **Install** button to start installation.#
4. Log in to the product as a user who has the Admin role and execute the `importservicetemplate` command to import the JP1/AO service templates or Service Template Set into JP1/AO.
5. If necessary, apply updates to the components used in the service template and changes to the service template to the service.

#

During installation using the Hitachi Program Product Installer, no installation wizard is displayed. For details about how to use the Hitachi Program Product Installer, see 1.3.2 Installation procedure using the Hitachi Program Product Installer. When installation by the Hitachi Program Product Installer finishes, perform step 4.

Results of procedure

- The following product name is displayed in the Programs and Features window displayed by clicking Windows **Control Panel**, **Programs** and then **Programs and Features**.

  Product name:

  JP1/Automatic Operation Content Pack

  Version:

  vv.rr.mm
- Service Template Set is stored in the following folder:

  In Windows:

  JP1/AO-Content-Pack-installation-folder\contents\setup

  In Linux:

  /opt/jp1aocontset/contents/setup

To check whether a service template has been imported, use the list of service templates displayed in the **Service Template** window or execute the `listservices` command.

Related topics

- Updating the components used in a service template in the JP1/AO Administration Guide
- Applying service template changes to services in the JP1/AO Administration Guide

7 Uninstallation

This chapter explains how to uninstall JP1/AO.

7.1 Uninstallation procedure

Uninstall JP1/AO and related products.

Important

When JP1/AO is uninstalled, the files listed below contained in the JP1/AO installation folder, if any, are automatically deleted. If you do not want to delete these files, back them up or move them.

- SSL server certificate file used for HTTPS connections
- Private key files used for HTTPS connections
- Private key files used for public key authentication for SSH connections

The uninstallation procedure consists of the following steps.

Table 7-1: Uninstallation procedure

Task		Required/ optional	Reference
1	Prepare for uninstallation.	Required	7.2 Prepare for uninstallation
2	Uninstall JP1/AO and related products.	Required	For non-cluster systems: 7.3 Procedure to uninstall JP1/AO (non-cluster system) For cluster systems: 7.4 Procedure to uninstall JP1/AO (cluster system)

Do not install other products during the uninstallation of JP1/AO.

7.2 Prepare for uninstallation

Before you uninstall JP1/AO, you must cancel or change various settings.

To prepare for uninstallation:

Log in as a user with the JP1/AO Admin role and either administrator or root permissions, and then perform the following tasks:

- Stop any security monitoring software, virus detection software, or process monitoring software.
  If such software is running, executing processes might be blocked, causing uninstallation to fail.
- If a Hitachi Command Suite product service is running, stop it.
  If you start the uninstallation with a Hitachi Command Suite product service running, it will display a dialog box prompting you to stop the service.
- Set **Startup type** for the JP1/AO service to **Automatic** or **Manual**.
  During uninstallation in Windows, if the **Startup type** of services related to JP1/AO is **Disabled**, uninstallation will fail because the service cannot be started. Set **Startup type** to **Automatic** or **Manual**.
  For details about the relevant services, see *JP1/AO services* in the *JP1/AO Administration Guide*.
- If automatic startup of JP1/AO at OS starts is enabled on Linux, cancel the automatic startup setting.

Related topics

- 2.9 Settings for automatically starting JP1/AO when the OS starts (in Linux)
- 7.1 Uninstallation procedure
- 7.3 Procedure to uninstall JP1/AO (non-cluster system)
- 7.4 Procedure to uninstall JP1/AO (cluster system)

7.3 Procedure to uninstall JP1/AO (non-cluster system)

The JP1/AO uninstallation procedure differs depending on the OS. In Windows, use **Programs and Features** in the **Control Panel**. In Linux, use the Hitachi Program Product Installer. When uninstallation using the Hitachi Program Product Installer finishes, perform step 4.

To uninstall JP1/AO:

1. Perform uninstallation as follows:

   If the OS is Windows:

   In the **Control Panel**, click **Programs**, and then **Programs and Features**. In the window that appears, select JP1/AO, and then click **Uninstall**.

   If the OS is Linux:

   Set the Hitachi Program Product Installer. For details about how to use the Hitachi Program Product Installer, see 1.3.2 Installation procedure using the Hitachi Program Product Installer.

2. Specify whether to start services after uninstallation is complete, as prompted by the wizard.[#1]
3. Uninstall JP1/AO.
4. Uninstall JP1/AO - Contents and JP1/AO Content Pack.[#2]

#1

During uninstallation using the Hitachi Program Product Installer, no wizard is displayed.

#2

For Hitachi Program Product Installer, if you uninstall JP1/AO, JP1/AO - Contents will be uninstalled at the same time.

If the following warning dialog box appears while you are uninstalling, you must restart the system:

An attempt to uninstall has failed. An attempt to delete several files has failed. Reboot the system after uninstallation ends.

If you install Hitachi Command Suite products without restarting the system, there is a risk that files required for the operation of Hitachi Command Suite products might be deleted when the system restarts after installation.

> **Important**
>
> If Common Component is on a different server than JP1/AO, a warning message is output if an attempt to delete authentication data fails during the uninstallation. In this case, after confirming that Common Component is running, delete the authentication data by executing the `hcmds64intg` command.

Results of procedure

- **JP1_Automatic Operation** is removed from **All Programs** in the **Start** menu.
- In Windows, if Common Component is also uninstalled when JP1/AO is uninstalled, you do not need to unregister the programs from the firewall exceptions list. They are automatically unregistered. In Linux, manually unregister the programs.

Related topics

- 7.1 Uninstallation procedure
- 7.2 Prepare for uninstallation
- 7.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Pack

7.4 Procedure to uninstall JP1/AO (cluster system)

In a cluster system, you must uninstall JP1/AO from both the active server and standby server.

The procedure to uninstall JP1/AO consists of the following steps.

Table 7-2: Uninstallation procedure

Task		Required/ optional	Reference
1	Prepare for uninstallation.	Required	Windows: 7.4.1 Procedure to configure services before uninstallation (for a cluster system in Windows) Linux: 7.4.2 Procedure to configure resources before uninstallation (for a cluster system in Linux)
2	Uninstall JP1/AO and related products.	Required	7.4.3 Procedure to uninstall JP1/AO and related products (cluster system)
3	Delete the folders that have been created in the shared folder.	Required	7.4.4 Procedure to delete folders created in the shared folder (cluster system)
4	In Windows: Delete services from the cluster software.	Required	7.4.5 Procedure to delete services from the cluster software (for a cluster system in Windows)
	In Linux: Delete resources from the cluster software.	Required	7.4.6 Procedure to delete resources from the cluster software (for a cluster system in Linux)

Related topics

- 7.1 Uninstallation procedure
- 7.2 Prepare for uninstallation

7.4.1 Procedure to configure services before uninstallation (for a cluster system in Windows)

Configure services before uninstallation.

To uninstall JP1/AO, you must log in to the JP1/AO server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

To configure services before uninstallation:

1. In the **Tasks** window, check the tasks. If any tasks are in the execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
3. Use the cluster software to bring the above resource group online.
4. Use the cluster software to bring the services and scripts offline.

   If the Hitachi Command Suite products are installed, bring all services and scripts offline except for the following services:

- HiRDB/ClusterService _HD1

If the Hitachi Command Suite products are not installed, bring the following services and script offline:

- HAutomation Engine Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt Web SSO Service

5. On the active server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
6. Use the cluster software to bring the following services offline:
   - HiRDB/ClusterService _HD1
7. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
8. Use the cluster software to bring the above resource group offline.
9. Use the cluster software to bring the services and scripts offline.

   If the Hitachi Command Suite products are installed, bring all services and scripts offline except for the following services:

   - HiRDB/ClusterService _HD1

   If the Hitachi Command Suite products are not installed, bring the following services and script offline:

   - HAutomation Engine Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
10. On the standby server, execute the `hcmds64srv` command with the `/stop` option specified to stop the JP1/AO service.
11. Use the cluster software to bring the following services offline:
    - HiRDB/ClusterService _HD1
12. In the cluster software, suppress failover for the resource group.

    Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart does not occur if the resource fails. Perform this action for all services and scripts registered in the resource group in order to suppress failover.

7.4.2 Procedure to configure resources before uninstallation (for a cluster system in Linux)

This subsection describes how to configure resources before uninstallation.

Before uninstalling JP1/AO, make sure that you log in to the JP1/AO server as a user with root permissions on the OS and administrator permissions on the cluster.

To configure resources before uninstallation:

1. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Input, In Progress (with Error), In Progress (Terminating), or Long Running), stop execution of the tasks or wait until the task status changes to the ended status.
2. Use the cluster software to bring the resource group offline.
3. Use the cluster software to disable stopping and monitoring resources other than the following resources:
   - Shared disk
   - Logical host name
   - Logical IP address
4. Use the cluster software to bring the resource group online.

7.4.3 Procedure to uninstall JP1/AO and related products (cluster system)

This subsection describes how to uninstall JP1/AO and related products. When you uninstall JP1/AO, you must also uninstall JP1/AO - Contents and JP1/AO Content Pack.

To uninstall JP1/AO and related products:

1. Use the cluster software to move the resource group where the JP1/AO service is registered to the active server.
2. Uninstall JP1/AO from the active server.
   After uninstallation, manually delete any files remaining under the JP1/AO installation folder.
3. On the active server, uninstall JP1/AO - Contents and JP1/AO Content Pack.
   After uninstallation, manually delete any files remaining under the installation folders for JP1/AO - Contents and JP1/AO Content Pack.
4. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
5. Uninstall JP1/AO from the standby server.
   After uninstallation, manually delete any files remaining under the JP1/AO installation folder.
6. On the standby server, uninstall JP1/AO - Contents and JP1/AO Content Pack.
   After uninstallation, manually delete any files remaining under the installation folders for JP1/AO - Contents and JP1/AO Content Pack.

Related topics

- 7.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Pack

7.4.4 Procedure to delete folders created in the shared folder (cluster system)

Delete folders created in the shared folder.

To delete folders created in the shared folder (In Windows):

1. Delete the following folders created in the shared folder:

- *shared-folder-name*\jp1ao
- *shared-folder-name*\Base64#

#

If other Hitachi Command Suite products have been installed, do not delete this folder.

To delete folders created in the shared folder (In Linux):

1. Delete the following folders created in the shared folder:
   - *shared-folder-name*/jp1ao
   - *shared-folder-name*/Base64

7.4.5 Procedure to delete services from the cluster software (for a cluster system in Windows)

Delete services from the cluster software.

To delete services from the cluster software:

1. Use the cluster software to delete from the resource group any of the following script and services that are not used by other applications:
   - HAutomation Engine Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt Web SSO Service
   - HiRDB/ClusterService _HD1
2. If you want to continue to use the remaining services and scripts, use the cluster software to enable failover for the resource group.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if a resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.

7.4.6 Procedure to delete resources from the cluster software (for a cluster system in Linux)

This subsection describes how to delete resources from the cluster software.

To delete resources from the cluster software:

1. If the following resources are not used by other applications, use the cluster software to delete these resources from the resource group:
   - Database for Common Component
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service

- HBase 64 Storage Mgmt Web Service
- HAutomation Engine Web Service

2. To continue using the remaining resources, use the cluster software to enable starting, stopping, and monitoring the resources.

7.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Pack

After uninstalling JP1/AO, uninstall JP1/AO - Contents and JP1/AO Content Pack. If the OS is Windows, uninstall them manually. If the OS is Linux, uninstall them by using the Hitachi Program Product Installer.

Before you begin

Uninstalling JP1/AO - Contents and JP1/AO Content Pack deletes their installation folders completely. Back up any necessary user-created folders and files before uninstallation.

To uninstall JP1/AO - Contents and JP1/AO Content Pack:

1. Perform uninstallation as follows:

   If the OS is Windows:

   Click **Control Panel**, **Programs**, and then **Programs and Features**. Then, select **JP1/Automatic Operation - Contents** or **JP1/Automatic Operation Content Pack**, and then **Uninstall**.

   If the OS is Linux:

   Set the Hitachi Program Product Installer. For details about how to use the Hitachi Program Product Installer, see 1.3.2 Installation procedure using the Hitachi Program Product Installer.

2. Uninstall JP1/AO - Contents or JP1/AO Content Pack according to the wizard.#

#

During uninstallation using the Hitachi Program Product Installer, no wizard is displayed. When you uninstall JP1/AO, JP1/AO - Contents is also uninstalled.

Related topics

- 1.5.2 JP1/AO Content Pack installation folder

8 Server Migration

This chapter explains how to migrate the environment in JP1/AO.

8.1 JP1/AO system migration procedure (to an environment with the same host name or IP address)

To migrate a JP1/AO system to an environment with the same host name or IP address , you must perform a backup and restore operation.

Prerequisites

- The following items must match on the original server and the target server:
  - Host name
  - IP address
  - System locale
  - The environment for Hitachi Command Suite products (configuration, version number, revision number, and restriction code)
  - JP1/AO installation folder
  - JP1/AO installation folders for databases
- No tasks must be in the In Progress, Waiting for Response, Abnormal Detection, or Terminated status on the original JP1/AO server.
- JP1/AO must not be installed on the target server.

The following describes the migration procedure depending on whether the original JP1/AO server has been upgraded.

Table 8-1: Migration procedure

Task		Reference
1	Back up JP1/AO on the original server.	For non-cluster systems: *Backing up data in JP1/AO (non-cluster configuration)* in the *JP1/AO Administration Guide* For cluster systems: *Backing up data in JP1/AO (Windows cluster configuration)* or *Backing up data in JP1/AO (Linux cluster configuration)* in the *JP1/AO Administration Guide*
2	Install JP1/AO on the target server.	For non-cluster systems: 1.1 New installation procedure For cluster systems: 5.1 Procedure for installing JP1/AO in a cluster system
3	Restore JP1/AO on the target server.	For non-cluster systems: *Restoring data in a JP1/AO system (non-cluster configuration)* in the *JP1/AO Administration Guide* For cluster systems: *Restoring the JP1/AO system (Windows cluster configuration)* or *Restoring the JP1/AO system*

Task		Reference
3	Restore JP1/AO on the target server.	*(Linux cluster configuration)* in the *JP1/AO Administration Guide*
4	Make sure that the target server is running, and then start operations.	--

Legend:

--: None

8.2 JP1/AO system migration procedure (to an environment with a different host name or IP address)

To migrate a JP1/AO system to an environment with a different host name or IP address , you must change the host name or IP address of the target server to those of the original server. After restoring JP1/AO, reset the host name or IP address of the target server to the one before the change.

Prerequisites

- The following items must match on the original server and the target server:
  - Host name
  - IP address
  - System locale
  - The environment for Hitachi Command Suite products (configuration, version number, revision number, and restriction code)
  - JP1/AO installation folder
  - JP1/AO installation folders for databases
- No tasks must be in the In Progress, Waiting for Response, Abnormal Detection, or Terminated status on the original JP1/AO server.
- JP1/AO must not be installed on the target server.

The following describes the migration procedure depending on whether the original JP1/AO server has been upgraded.

Table 8-2: Migration procedure

Task		Reference
1	Back up JP1/AO on the original server.	For non-cluster systems: *Backing up data in JP1/AO (non-cluster configuration)* in the *JP1/AO Administration Guide* For cluster systems: *Backing up data in JP1/AO (Windows cluster configuration)* or *Backing up data in JP1/AO (Linux cluster configuration)* in the *JP1/AO Administration Guide*
2	Change the host name and IP address of the target server to match the migration source environment.	--
3	Install JP1/AO on the target server.	For non-cluster systems: 1.1 New installation procedure For cluster systems: 5.1 Procedure for installing JP1/AO in a cluster system
4	Restore JP1/AO on the target server.	For non-cluster systems: *Restoring data in a JP1/AO system (non-cluster configuration)* in the *JP1/AO Administration Guide*

Task		Reference
4	Restore JP1/AO on the target server.	For cluster systems: *Restoring the JP1/AO system (Windows cluster configuration)* or *Restoring the JP1/AO system (Linux cluster configuration)* in the *JP1/AO Administration Guide*
5	Return the host name and IP address of the target server to those before the migration. Perform the procedure for changing the host name and IP address.	• 4.3 Procedure to change the host name of the JP1/AO server • 4.4 Procedure to change the IP address of the JP1/AO server
6	Make sure that the target server is running, and then start operations.	--

Legend:

--: None

9 Troubleshooting During Setup

This chapter explains what to do if problems occur in JP1/AO.

9.1 What to do if you are unable to resolve the problem based on what is displayed in the error dialog box

If you are unable to resolve the problem based on what is displayed in the error dialog box, use the `hcmds64getlogs` command to collect log information, and check the logs for details of the problem.

In a cluster environment, be sure to collect log information on both the active and standby servers.

Appendix

A. Reference Information

This appendix provides information that is helpful for using JP1/AO.

A.1 List of folders (in Windows)

The table below lists the folders that are created when JP1/AO is installed in a Windows environment.

In the table, the default value for *JP1/AO-installation-folder* as shown below:

system-drive\Program Files\Hitachi\JP1AO

Table A-1: List of folders created during installation (in Windows)

Folder	Contents
JP1/AO-installation-folder\bin	Folder containing various commands
JP1/AO-installation-folder\conf	Folder for definition files used to set a JP1/AO environment
JP1/AO-installation-folder\contents	Service template folder
JP1/AO-installation-folder\data	Data folder
JP1/AO-installation-folder\develop	Folder for development service templates (plug-ins) and service template packages
JP1/AO-installation-folder\docroot	Folder for help files
JP1/AO-installation-folder\inst	Temporary working folder for installation and uninstallation
JP1/AO-installation-folder\lib	Folder for libraries
JP1/AO-installation-folder\logs	Log folder
JP1/AO-installation-folder\ossSource	Folder containing source files for open source software
JP1/AO-installation-folder\system	Folder for JP1/AO system files
JP1/AO-installation-folder\webapps	Working folder used by JP1/AO internal commands
JP1/AO-installation-folder\work	Working folder
system-drive\Program Files\Hitachi\HiCommand\Base64#	Common Component installation folder

#

If one or more Hitachi Command Suite products have already been installed, Common Component has already been installed in a folder that was created when the first Hitachi Command Suite product was installed. In such a case, therefore, this folder is not created.

A.2 List of folders (in Linux)

The following table lists the folders that are created when JP1/AO is installed in a Linux environment.

Table A-2: List of folders created during installation (in Linux)

Folder	Contents
/opt/jp1ao/bin	Folder containing various commands
/opt/jp1ao/conf	Folder for definition files used to set a JP1/AO environment
/var/opt/jp1ao/contents	Service template folder
/var/opt/jp1ao/data	Data folder
/var/opt/jp1ao/develop	Folder for development service templates (plug-ins) and service template packages
/opt/jp1ao/docroot	Folder for help files
/opt/jp1ao/inst	Temporary working folder for installation and uninstallation
/opt/jp1ao/lib	Folder for libraries
/var/opt/jp1ao/logs	Log folder
/opt/jp1ao/ossSource	Folder containing source files for open source software
/opt/jp1ao/system	Folder for JP1/AO system files
/opt/jp1ao/webapps	Working folder used by JP1/AO internal commands
/var/opt/jp1ao/work	Working folder
/opt/HiCommand/Base64	Common Component installation folder

A.3 Information necessary to perform operations on the scheduler services and embedded databases in a configuration in which JP1/AO coexists with JP1/AJS3

This appendix describes the information that is necessary to check and delete the scheduler services for JP1/AO, and to delete the embedded databases used by those scheduler services in a configuration in which JP1/AO coexists with JP1/AJS3.

Note that the information described here is contained in the config_system.properties file. The following table lists the location of this file.

Table A-3: Location of the config_system.properties file

Item	Location
File used for reference in an environment in which JP1/AO is installed	In Windows: *JP1/AO-installation-folder*\conf In Linux: /opt/jp1ao/conf
File used to restore JP1/AO with backup data	*folder-containing-backup-data*\Automation\conf

Information necessary to check the scheduler service for JP1/AO:

To check whether the scheduler service for JP1/AO exists, execute the `ajsembdbidlist` command.

When executing this command, specify the name of the scheduler service for JP1/AO. The scheduler service name that you specify in the command is the value of the task.ajs.serviceName= entry in the config_system.properties file.

The following table lists the information about the scheduler service for JP1/AO to be specified in the `jajs_setup` command.

Table A-4: Information about the scheduler service for JP1/AO to be specified in the `jajs_setup` command

Option	Explanation	Value to be specified
`-a`	Specifies that a scheduler service will be added.	Do not specify a value.
`-F`	Specifies the name of a scheduler service.	The value of task.ajs.serviceName= in the config_system.properties file
`-n`	Specifies the identification number of the scheduler service.	The value of external.ajs.serviceid= in the config_system.properties file
`-p`	Specifies the service name of the job status communication port.	The value of external.ajs.jobportname= in the config_system.properties file
`-d`	Specifies the name of the database directory.	In Windows: *JP1/AO-installation-folder*\system\extajs\database\schedule*scheduler-service-name* In Linux: /opt/jp1ao/system/extajs/database/schedule/*scheduler-service-name*
`-t`	Specifies the name of the temporary directory.	In Windows: *JP1/AO-installation-folder*\system\extajs\tmp*scheduler-service-name* In Linux: /opt/jp1ao/system/extajs/tmp/*scheduler-service-name*
`-j`	Specifies the name of the job information directory.	In Windows: *JP1/AO-installation-folder*\system\extajs\jobinf*scheduler-service-name* In Linux: /opt/jp1ao/system/extajs/jobinf/*scheduler-service-name*
`-b`	Specifies the name of the directory for backup information.	In Windows: *JP1/AO-installation-folder*\system\extajs\backup*scheduler-service-name* In Linux: /opt/jp1ao/system/extajs/backup/*scheduler-service-name*
`-I`	Specifies the setup identifier.	The value of external.ajs.dbid= in the config_system.properties file
`-P`	Specifies the port number for the embedded database.	The value of external.ajs.dbport= in the config_system.properties file
`-M`	Specifies the database model.	The value of external.ajs.dbsize= in the config_system.properties file

Information necessary to delete the scheduler service for JP1/AO:

To delete the scheduler service for JP1/AO, execute the `jajs_setup` command, specifying the name of the scheduler service.

The scheduler service name that you specify in the command is the value of task.ajs.serviceName= in the config_system.properties file.

Information necessary to delete the embedded database used by the scheduler service for JP1/AO:

To delete the embedded database used by the scheduler service for JP1/AO, execute the `ajsembdbuninstl` command, specifying the setup identifier.

The setup identifier that you specify in the command is the value of external.ajs.dbid= in the config_system.properties file.

Related topics

- jajs_setup in the manual JP1/Automatic Job Management System 3 Command Reference
- ajsembdbuninstl in the manual JP1/Automatic Job Management System 3 Command Reference
- ajsembdbidlist in the manual JP1/Automatic Job Management System 3 Command Reference
- jajs_config in the manual JP1/Automatic Job Management System 3 Command Reference

A.4 Version changes

(1) Changes in version 12-60

- Windows Server 2022 was added as a supported operating system.
- Notes were added regarding the use of products that use the same Common Component.
- The import of the service template provided by JP1/AO - Contents was added to the installation procedure.
- The description of the files to be copied was changed.
- Notes were added to the procedure for enabling the HTTPS connection between a web browser and JP1/AO.
- The following operating systems are now supported:
  - Red Hat Enterprise Linux 8
  - Oracle Linux 8
  - CentOS 8
- The format of the private key was added to the tips in the procedure for creating public and private keys.
- The following items were added as setting items in the user-specified properties file (config_user.properties):
  - plugin.adapter.timeout
  - task.periodicalTaskArchive.enable
  - task.periodicalTaskArchive.period
  - task.periodicalTaskArchive.taskCountThreshold
  - task.periodicalTaskArchive.taskCountAfterArchive
  - task.execute.skip.serverStart
  - plugin.wmi.win32.UACAdministratorsExec
  - plugin.wmi.win32.CreationFlags.CREATE_NO_WINDOW
- Descriptions of the following items, as setting items in the connection-destination property file, were changed:
  - wmi.workDirectory.sharedName

    - wmi.adapter.id
- The following items were added as setting items in the connection-destination property file:
    - wmi.win32.UACAdministratorsExec
    - wmi.win32.CreationFlags.CREATE_NO_WINDOW
- The encryption method for connecting to the LDAP directory server was added.
- Changes were made to the procedure (when the JP1/AO server is using Linux) for configuring settings to automatically start the JP1/AO service at the startup of the OS.
- A security configuration operation was added to the flow of tasks for linking with Active Directory.
- Descriptions of security settings for communication with the LDAP directory server were added.
- Descriptions of the definition files used for linking with JP1/IM were changed.
- Task confirmation was added to the procedure for changing the host name of the JP1/AO server.
- Notes on changing port numbers were added.
- The procedure for changing a port number was added.
- The procedure for performing an overwrite or upgrade installation was changed.
- The procedure for enabling failover of a resource group was changed.
- The procedure for changing resource settings was changed.
- The procedure for performing an overwrite installation of JP1/AO Content Pack was changed.
- A description of how to prepare for uninstallation was added.
- The prerequisite conditions for replacing a JP1/AO system were changed.

(2) Changes in version 12-01

- Additions and changes were made to the procedures for specifying the settings that automatically start the JP1/AO services when the OS starts, when the JP1/AO server is running in Linux.

(3) Changes in version 12-00

- None

(4) Changes in version 11-50

- The procedure for enabling HTTPS connections was changed.
- The timing for applying the definitions of the user-specified properties file was changed.
- The following properties were added to the user-specified properties file: plugin.stdoutSize.wmi, plugin.stdoutSize.ssh, plugin.stdoutSize.telnet, and server.http.port.
- The default value for the property notification.jp1event in the user-specified properties file was changed to false.
- The property task.ajs.IPBindhost was deleted from the user-specified properties file.
- The property server.http.port was added to the items that need to be set to change the communication port while the communication method is HTTP.
- The procedure for changing the host name of the JP1/AO server was changed.
- The description of the procedure for changing the maximum number of plug-ins that can be executed concurrently was changed.

(5) Changes in version 11-10

- The installation of .NET Framework is no longer required when the OS is Windows Server 2012 or Windows Server 2012 R2, and descriptions of this requirement were deleted.
- JP1/AO no longer requires JP1/Base as a prerequisite product, and descriptions of this requirement were deleted.
- JP1/AO no longer uses JP1/AJS3 as a task processing engine, and content indicating otherwise was deleted.
- Adobe Flash Player is no longer required, and descriptions of this requirement were deleted.
- A procedure for importing the SSL server certificate into the truststore of Common Component was added.
- A note on the procedure for importing the SSL server certificate into the truststore of Common Component was added.
- The task monitor properties client.monitor.tasklog.maxfilesize and client.monitor.status.interval were deleted from the setting items in the user-specified properties file.
- The uninstallation of JP1/AO is no longer required when changing a host name for a cluster system. Accordingly, the procedure was updated.
- Hitachi Automation Director was added as a product that cannot be installed on a device on which JP1/AO is installed.
- A list of required OSs for JP1/AO was deleted.
- JP1/AJS3 is no longer included in JP1/AO, and therefore the `stopcluster` command is no longer required. Accordingly, descriptions of this requirement were deleted.
- The folder path of Common Component created on the shared disk of JP1/AO was changed.
- The task of uninstalling JP1/Base was added for when JP1/Base is not used after upgrading JP1/AO from a version earlier than 11-10 to version 11-10 or later.
- The following tasks were added: post-upgrade tasks required for when automatic startup for JP1/AJS3 is enabled and an environment in which JP1/AO coexists with JP1/AJS3 is used.
- The JP1/AO installation folder was added to items that require consistency between the replacement-source server and replacement-destination server.
- The host name, IP address, and JP1/AO installation folder were added to the items that require consistency between the replacement-source server and replacement-destination server.

(6) Changes in version 11-01

- The procedure for automatically starting JP1/AO at OS startup in an environment where JP1/AO and JP1/AJS3 coexist was added.
- A cautionary note was added warning that you cannot specify a symbolic link as the installation destination when performing a new installation of JP1/AO in Linux.
- The default database folder for the Common Component was added.
- The procedure for enabling https connections and the default contents of the user_httpsd.conf file were changed.
- A cautionary note was added warning that the JP1/AO login window will not appear if the connection between the Web browser and JP1/AO is configured incorrectly.
- The procedure for importing an SSL server certificate into the Common Component was added. This certificate is required for https connections between JP1/AO and external Web servers.
- The description of the client.events.refreshinterval and client.editor.upload.maxfilesize properties in the user-specified properties file was changed.

(7) Changes in version 11-00

(a) Changes from the manual (3021-3-082-70)

- The following operating systems are now supported:
  - Linux 7
  - Oracle Linux 6 (x64)
  - Oracle Linux 7
  - CentOS 6 (x64)
  - CentOS 7
  - SUSE Linux 12
- The following operating systems are no longer supported:
  - Linux 5 (AMD/Intel 64)
  - Linux 5 Advanced Platform (AMD/Intel 64)
- The product was migrated from 32-bit Windows to 64-bit Windows.
- The installation folder was changed for the Windows version of JP1/AO and the Common Component.
- A description of using JP1/AO in English and Chinese-language environments was added.
- The port numbers used for communication between JP1/AO and Web browsers were changed.
- JP1/AO can now coexist with JP1/AJS3 version 11.
- Hitachi Automation Director was added as a conflicting product for JP1/AO.
- A description of the language settings in the JP1/AO server OS was added.
- The folders that cannot be specified as the installation destination of JP1/AO were changed.
- Items that can be specified in the user-specified properties file (config_user.properties) were added.
- Items that can be specified in the connection-destination property file (connection-destination-name.properties) were added.
- Tasks required before and after upgrade installation were added.
- Service groups were added as a way to manage resources. Accordingly, resource groups were removed.

(b) Changes from the manual (3021-3-313-20(E))

- Linux was added as a supported operating system.
- The installation folder was changed for the Windows version of JP1/AO and the Common Component.
- The port numbers used for communication between JP1/AO and Web browsers were changed.
- The product was migrated from 32-bit Windows to 64-bit Windows.
- Keyboard interactive authentication was added as an authentication method used for SSH connections with operation target devices.
- Items that can be specified in the user-specified properties file (config_user.properties) were added.
- Items that can be specified in the connection-destination property file (connection-destination-name.properties) were added.
- The procedure to change the maximum number of plug-ins that can be executed concurrently was added.

- Descriptions about how to specify whether to back up the database and how to specify the folder in which the database is to be backed up were added.
- A prerequisite that the restriction code of the Hitachi Command Suite products must match on the original server and the target server was added.
- JP1/AO can now coexist with JP1/AJS3 version 11.
- Hitachi Automation Director was added as a conflicting product for JP1/AO.
- A description of the language settings in the JP1/AO server OS was added.
- The folders that cannot be specified as the installation destination of JP1/AO were changed.
- Tasks required before and after upgrade installation were added.
- Service groups were added as a way to manage resources. Accordingly, resource groups were removed.

(8) Changes in version 10-52

(a) Changes in the manual (3021-3-082-70)

- Linux was added as a supported operating system.
- Keyboard interactive authentication was added as an authentication method used for SSH connections with operation target devices.
- The plugin.localMode property used to specify whether to use the local execution function was added to the property file (config_user.properties).
- The plugin.threadPoolSize property used to specify the maximum number of plug-ins that can be executed concurrently was added to the property file (config_user.properties).
- The procedure to change the maximum number of plug-ins that can be executed concurrently was added.
- Descriptions about how to specify whether to back up the database and how to specify the folder in which the database is to be backed up were added.
- A prerequisite that the restriction code of the Hitachi Command Suite products must match on the original server and the target server was added.

(9) Changes in version 10-50

(a) Changes in the manual (3021-3-082-60)

- The HTTPS protocol can now be used to establish a connection between a JP1/AO server and a Web browser.
- Public key authentication was added as an authentication method used with operation target devices.
- It is now possible to specify an IP address for the `task.ajs.IPBindhost` property key in the property file (config_user.properties).
- The ssh.privateKeyFile property used to specify the absolute path of the private key file for public key authentication was added to the property file (config_user.properties).
- The plugin.remoteFileAccess.retry.times property used to specify the number of retries for a remote file manipulation command was added to the property file (config_user.properties).
- Active Directory linkage was added as external authentication linkage.
- A description about the configuration file for external authentication server linkage (exauth.properties) used to specify the settings required for external authentication linkage was added.
- The `stopcluster` command was added.

Preparation for stopping the JP1/AO service in a cluster environment is now possible.

- A cautionary note relating to if the following files are stored in the JP1/AO installation folder was added:
  - SSL server certificate files used for HTTPS connections
  - Private key files used for HTTPS connections
  - Private key files used for public key authentication in SSH connections

(b) Changes in the manual (3021-3-313-20(E))

- For the manual issued in December 2014 or later, the title and reference number were changed as shown below.

  Before the change:

  Job Management Partner 1/Automatic Operation GUI and Command Reference (3021-3-315(E))

  After the change:

  Job Management Partner 1/Automatic Operation GUI, Command, and API Reference (3021-3-366(E))
- Windows Server 2012 R2 was added as an applicable operating system.
- The HTTPS protocol can now be used to establish a connection between a JP1/AO server and a Web browser.
- Public key authentication was added as an authentication method used with operation target devices.
- The action to be taken if more time is required to complete a task in an environment where external networks cannot be connected was added.
- The following property keys were added to the property file (config_user.properties):
  - task.details.jobnet.status.visible
  - packagemanager.extraPresets.maxFiles
  - ssh.privateKeyFile
  - plugin.remoteCommand.executionDirectory.wmi
  - plugin.remoteCommand.executionDirectory.ssh
  - plugin.remoteCommand.workDirectory.ssh
  - plugin.remoteFileAccess.retry.times
  - server.editor.step.perTemplate.maxnum
  - server.editor.step.perLayer.maxnum
  - client.editor.canvas.maxwidth
  - client.editor.canvas.maxhigh
  - tasklist.debugger.autodelete.taskRemainingPeriod
  - client.debugger.tasklog.maxfilesize
  - logger.debugger.TA.MaxFileSize
  - client.monitor.tasklog.maxfilesize
  - client.monitor.tasklog.refresh.interval
  - client.monitor.status.interval
- The default value of the `logger.TA.MaxFileSize` property key in the property file (config_user.properties) was changed to 10240.
- It is now possible to specify an IP address for the `task.ajs.IPBindhost` property key in the property file (config_user.properties).

- A definition example of the connection-destination property file was added.
- `ibm-943` was changed to `ibm-943C` as a specifiable value for the `terminal.charset` key in the connection destination property file, and as a character set that can be specified in the character set mapping file.
- The character sets that can be specified in the character set mapping file were added.
- A description about the configuration file for external authentication server linkage (exauth.properties) used to specify the settings required for external authentication linkage was added.
- Active Directory linkage was added as external authentication linkage.
- The `stopcluster` command was added.

  Preparation for stopping the JP1/AO service in a cluster environment is now possible.
- The step for starting the JP1/Base service was deleted from the procedure for changing the IP address of the JP1/AO server.
- A folder for service templates and plug-ins that are in the process of development was added.
- A cautionary note relating to the upgrade installation procedure was added.
- A cautionary note relating to if the following files are stored in the JP1/AO installation folder was added:
  - SSL server certificate files used for HTTPS connections
  - Private key files used for HTTPS connections
  - Private key files used for public key authentication in SSH connections

(10) Changes in version 10-12

(a) Changes in the manual (3021-3-082-50)

- Windows Server 2012 R2 was added as an applicable operating system.
- The default value of the `logger.TA.MaxFileSize` property key in the property file (config_user.properties) was changed to 10240.
- The following property keys were added to the property file (config_user.properties):
  - task.details.jobnet.status.visible
  - packagemanager.extraPresets.maxFiles
  - plugin.remoteCommand.executionDirectory.wmi
  - plugin.remoteCommand.executionDirectory.ssh
  - plugin.remoteCommand.workDirectory.ssh
  - tasklist.debugger.autodelete.taskRemainingPeriod
  - client.debugger.tasklog.maxfilesize
  - logger.debugger.TA.MaxFileSize
  - client.monitor.tasklog.maxfilesize
  - client.monitor.tasklog.refresh.interval
  - client.monitor.status.interval
- A folder for service templates and plug-ins that are in the process of development was added.

(11) Changes in version 10-11

(a) Changes in the manual (3021-3-082-40)

- The following property keys were added to the property file (config_user.properties):
  - server.editor.step.perTemplate.maxnum
  - server.editor.step.perLayer.maxnum
  - client.editor.canvas.maxwidth
  - client.editor.canvas.maxhigh
- `ibm-943` was changed to `ibm-943C` as a specifiable value for the `terminal.charset` key in the connection destination property file, and as a character set that can be specified in the character set mapping file.
- A definition example of the connection-destination property file was added.
- The character sets that can be specified in the character set mapping file were added.
- The action to be taken if more time is required to complete a task in an environment where external networks cannot be connected was added.
- The step for starting the JP1/Base service was deleted from the procedure for changing the IP address of the JP1/AO server.
- A cautionary note relating to the upgrade installation procedure was added.

(12) Changes in version 10-10

(a) Changes in the manual (3021-3-082-30)

- *JP1/Automatic Operation Service Template Developer's Guide* was added as a supplied manual.
- A definition example of the character-set mapping file (charsetMapping_user.properties) was added.
- The role and permissions on JP1/AO were added in the description defining permission levels in JP1/Base (JP1/Base link).
- Precautions related to the upgrade installation procedure were added.

(b) Changes in the manual (3021-3-313-10(E))

- The requirement for installation of .NET Framework 3.5 in Windows Server 2012 was added.
- *Job Management Partner 1/Automatic Operation Service Template Developer's Guide* was added as a supplied manual. In addition, a folder was added for English manuals.
- Email notification files now support Chinese environments in addition to the English and Japanese environments.
- The connection-destination property file (*connection-destination*.properties) was added.
- The character-set mapping file (charsetMapping_user.properties) was added.
- The following property keys were added to the property file (config_user.properties):
  - telnet.port.number
  - plugin.terminal.prompt.account
  - plugin.terminal.prompt.password
  - telnet.connect.wait
  - telnet.connect.retry.times

    - telnet.connect.retry.interval
    - logger.Audit.command.useLoginUserID
- The role and permissions on JP1/AO were added in the description defining permission levels in JP1/Base (JP1/Base link).
- The definition files that are used for linkage with JP1/IM now support English and Chinese environments in addition to the Japanese environment.
- Descriptions about how to link JP1/AO with JP1/AJS3 were added.
- The procedure for stopping JP1/Base services was deleted from the procedure for changing the IP address of the JP1/AO server.
- The section that describes setting up a cluster system was moved from Chapter 1 to Chapter 5.
- Descriptions about an overwrite installation of JP1/AO Content Set were added.
- A description of an upgrade installation was added.
- Precautions related to the upgrade installation procedure were added.

(13) Changes in version 10-02

(a) Changes in the manual (3021-3-082-20)

- The requirement for installation of .NET Framework 3.5 in Windows Server 2012 was added.
- The connection-destination property file (*connection-destination*.properties) was added.
- The character-set mapping file (charsetMapping_user.properties) was added.
- The following property keys were added to the property file (config_user.properties):
    - telnet.port.number
    - plugin.terminal.prompt.account
    - plugin.terminal.prompt.password
    - telnet.connect.wait
    - telnet.connect.retry.times
    - telnet.connect.retry.interval
    - logger.Audit.command.useLoginUserID
- Descriptions about how to link JP1/AO with JP1/AJS3 were added.
- The section that describes setting up a cluster system was moved from Chapter 1 to Chapter 5.
- Descriptions about an overwrite installation of JP1/AO Content Set were added.
- A description of an upgrade installation was added.

(14) Changes in version 10-01

(a) Changes in the manual (3021-3-082-10)

- None

Index

A

C

D

E

F

H

I

J

L

M

N

O

P

R

S

T

U

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan