Job Management Partner 1 Version 10

Job Management Partner 1/Automatic Operation Configuration Guide

3021-3-313-20(E)

Notices

■ Relevant program products

P-242C-E1AL Job Management Partner 1/Automatic Operation 10-50 (for Windows Server 2008 R2,Windows Server 2012,Windows Server 2012 R2)

The above product includes the following:

- P-CC242C-EAAL Job Management Partner 1/Automatic Operation - Server 10-50 (for Windows Server 2008 R2,Windows Server 2012,Windows Server 2012 R2)
- P-CC242C-EBAL Job Management Partner 1/Automatic Operation - Contents 10-50 (for Windows Server 2008 R2,Windows Server 2012,Windows Server 2012 R2)

P-F242C-E1AL1 Job Management Partner 1/Automatic Operation Contents Set 10-50 (for Windows Server 2008 R2,Windows Server 2012,Windows Server 2012 R2)

■ Trademarks

Active Directory is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Adobe and Flash Player are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

HP-UX is a product name of Hewlett-Packard Development Company, L.P. in the U.S. and other countries.

IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Intel is a trademark of Intel Corporation in the U.S. and/or other countries.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.

Itanium is a trademark of Intel Corporation in the United States and other countries.

Kerberos is a name of network authentication protocol created by Massachusetts Institute of Technology.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft .NET is software for connecting people, information, systems, and devices.

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Netscape is a trademark of AOL Inc.in the U.S. and other countries.

The OpenStack(R) Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

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

Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.

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

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc., in the United States and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

HITACHI
Inspire the Next

Hitachi, Ltd.

Java™ COMPATIBLE ENTERPRISE EDITION

Java™ COMPATIBLE

■ Issued

Dec. 2014: 3021-3-313-20(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-313-20(E)) and product changes related to this manual.

Changes	Location
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 a supported operating system.	1.1, 1.2.4, 5.2
HTTPS connection was added as a communication protocol available for JP1/AO servers and Web browsers.	1.1, 1.6, 2.4, 4.6.1
Public key authentication was added as an authentication method used with operation target devices.	1.1, 1.7, 2.2
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.	2.1, 2.9
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	2.2
The default value of the `logger.TA.MaxFileSize` property key in the property file (config_user.properties) was changed to 10240.	2.2

Changes	Location
It is now possible to specify an IP address for the `task.ajs.IPBindhost` property key in the property file (config_user.properties).	2.2
A definition example of the connection-destination property file was added.	2.6
`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.	2.6, 2.7
The character sets that can be specified in the character set mapping file were added.	2.7
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.	2.8
Active Directory linkage was added as external authentication linkage.	2.8, 3.2
The `stopcluster` command was added. Preparation for stopping the JP1/AO service in a cluster environment is now possible.	4.4.2, 5.3.6, 5.4.6, 6.3.2, 6.3.5, 8.4.1, 8.4.4
The step for starting the JP1/Base service was deleted from the procedure for changing the IP address of the JP1/AO server.	4.5.1
A folder for service templates and plug-ins that are in the process of development was added.	5.6, A.1
A cautionary note relating to the upgrade installation procedure was added.	7.1
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	8.1

Preface

This manual describes how to set up Job Management Partner 1/Automatic Operation.

In this manual, Job Management Partner 1 is abbreviated to *JP1*, and Job Management Partner 1/Automatic Operation is abbreviated to *JP1/AO*.

For reference information on JP1/AO manuals and a glossary, see the manual*Job Management Partner 1/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 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
.NET Framework	.NET Framework 3.5			Microsoft(R) .NET Framework 3.5
Active Directory				Microsoft(R) Active Directory
Hyper-V				Microsoft(R) Hyper-V(R)
Internet Explorer	Microsoft Internet Explorer			Microsoft(R) Internet Explorer(R)
	Windows Internet Explorer			Windows(R) Internet Explorer(R)
Windows	Windows 7			Microsoft(R) Windows(R) 7 Enterprise
				Microsoft(R) Windows(R) 7 Professional
				Microsoft(R) Windows(R) 7 Ultimate
	Windows Server 2003[#1]	Windows Server 2003[#1]		Microsoft(R) Windows Server(R) 2003, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003, Standard Edition
		Windows Server 2003 (x64)		Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Windows Server 2003 R2[#2]	Windows Server 2003 R2[#2]	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard Edition

Abbreviation				Full name or meaning
Windows	Windows Server 2003[#1]	Windows Server 2003 R2[#2]	Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
	Windows Server 2008	Windows Server 2008 R2	Windows Server 2008 R2 Datacenter	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
			Windows Server 2008 R2 Enterprise	Microsoft(R) Windows Server(R) 2008 R2 Enterprise
			Windows Server 2008 R2 Standard	Microsoft(R) Windows Server(R) 2008 R2 Standard
		Windows Server 2008 x64	Windows Server 2008 Datacenter x64	Microsoft(R) Windows Server(R) 2008 Datacenter x64
			Windows Server 2008 Enterprise x64	Microsoft(R) Windows Server(R) 2008 Enterprise x64
			Windows Server 2008 Standard x64	Microsoft(R) Windows Server(R) 2008 Standard x64
		Windows Server 2008 x86	Windows Server 2008 Datacenter x86	Microsoft(R) Windows Server(R) 2008 Datacenter x86
			Windows Server 2008 Enterprise x86	Microsoft(R) Windows Server(R) 2008 Enterprise x86
			Windows Server 2008 Standard x86	Microsoft(R) Windows Server(R) 2008 Standard x86
	Windows Server 2012	Windows Server 2012 Datacenter		Microsoft(R) Windows Server(R) 2012 Datacenter
		Windows Server 2012 Standard		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Windows Server 2012 R2 Datacenter		Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Windows Server 2012 R2 Standard		Microsoft(R) Windows Server(R) 2012 R2 Standard
	Windows Server Failover Cluster			Microsoft(R) Windows Server(R) Failover Cluster
	Windows Vista			Microsoft(R) Windows Vista(R) Business
				Microsoft(R) Windows Vista(R) Enterprise
				Microsoft(R) Windows Vista(R) Ultimate
	Windows XP			Microsoft(R) Windows(R) XP Professional Operating System

#1

In descriptions, if Windows Server 2003 (x64) or Windows Server 2003 R2 is noted alongside Windows Server 2003, the description for Windows Server 2003 does not apply to Windows Server 2003 (x64) or Windows Server 2003 R2.

#2

In descriptions, if Windows Server 2003 R2 (x64) is noted alongside Windows Server 2003 R2, the description for Windows Server 2003 R2 does not apply to Windows Server 2003 R2 (x64).

■ 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.
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 are represented as follows:

JP1/AO installation folder:
system-drive\Program Files (x86)\Hitachi\JP1AO

Common Component installation folder:
system-drive\Program Files (x86)\Hitachi\HiCommand\Base

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 and installing JP1/Base, 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	Install JP1/Base on the JP1/AO server (the server on which you plan to install JP1/AO).	Required	1.2.2 Installing JP1/Base
3	You must register a JP1 user before you can install JP1/AO. If you want to use a user other than jp1admin or a user who is not yet defined in the existing JP1/Base, create the desired JP1 user in JP1/Base.	Optional	1.2.3 Creating a JP1 user in JP1/Base
4	If the OS at the JP1/AO installation destination is Windows Server 2012 or Windows Server 2012 R2, you must install .NET Framework 3.5. If the OS is Windows Server 2008, .NET Framework 3.5 is installed by default.	Optional	1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2)
5	Perform a new installation of JP1/AO from the distribution media.	Required	1.3.1 Procedure to perform a new installation of JP1/AO
6	Install the manual on the JP1/AO server.	Optional	1.4 Procedure to install the manual
7	Install JP1/AO Content Set.	Optional	1.5.1 Procedure to install JP1/AO Content Set
8	Enable HTTPS connections between Web browsers and JP1/AO servers.	Optional	1.6 Procedure to enable HTTPS connections between Web browsers and JP1/AO
9	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.

- Before you start the installation of JP1/AO, uninstall the following products that conflict with JP1/AO:
  - JP1/AJS3 - Manager
  - JP1/AJS3 - Agent
  - JP1/AJS2 - Manager
  - JP1/AJS2 - Agent
- Log in to the JP1/AO server as a user with Administrators permissions and check the following:
  - 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.
- Stop any security monitoring software, virus detection software, or process monitoring software.

  If such software is running, installation might fail.
- Set **Startup Type** for the following services to **Automatic** or **Manual**: Different services are provided depending on whether JP1/Base is installed on the JP1/AO server, whether Hitachi Command Suite products are installed on the JP1/AO server, and whether an overwrite installation of JP1/AO is performed.

Service name	JP1/Base is installed on the JP1/AO server	Hitachi Command Suite products are installed on the JP1/AO server	Overwrite installation of JP1/AO is performed
HAutomation Engine	N	N	Y
HAutomation Engine Database _JF0	N	N	Y
HAutomation Engine Web Service	N	N	Y
HiRDB/EmbeddedEdition _HD0	N	Y	Y
HBase Storage Mgmt Common Service	N	Y	Y
HBase Storage Mgmt Web Service	N	Y	Y
HBase Storage Mgmt Web SSO Service	N	Y	Y
JP1/Base (HAutomation Common Base)	Y	N	Y
JP1/Base Control Service (HAutomation Common Control Service)	Y	N	Y
JP1/Base Event (HAutomation Common Event)	Y	N	Y

1. New Installation

Service name	JP1/Base is installed on the JP1/AO server	Hitachi Command Suite products are installed on the JP1/AO server	Overwrite installation of JP1/AO is performed
JP1/Base EventlogTrap (HAutomation Common EventlogTrap)	Y	N	Y
JP1/Base LogTrap (HAutomation Common LogTrap)	Y	N	Y

Legend:

Y: Provided. N: Not provided.

When you perform an installation in Windows, if the startup type of the JP1/AO service is **Disabled**, that service cannot be started and installation will fail. Set **Startup Type** to **Automatic** or **Manual**.

For details about the JP1/AO service, see *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*.

- 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.
- When you install JP1/AO, the JP1/Base services are started. If you are controlling the order in which services start in JP1/Base, make sure that there is no problem during service startup.
- Before you run the installation, close any open command prompts.

  If you do not close the command prompts before installing, the environment variable settings that you set during installation will not be applied.
- If the Hitachi Command Suite products are installed, stop the Hitachi Command Suite services.

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

  Note that users and user groups that are created in JP1/AO will be shared with the Hitachi Command Suite products and can take advantage of the single sign-on functionality.

Related topics

- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- 3.3.1 Procedure to enable single sign-on to Hitachi Command Suite products
- *Functions for linking with other products* in the *Job Management Partner 1/Automatic Operation Overview and System Design Guide*

1.2.2 Installing JP1/Base

Install JP1/Base, which is a prerequisite product, on the JP1/AO server.

Related topics

- *Installation and Setup* in the *Job Management Partner 1/Base User's Guide*

1.2.3 Creating a JP1 user in JP1/Base

To install JP1/AO, the JP1 users must be registered in advance. Make sure that there is at least one JP1 user, and that the user mapping has been done.

To use a jp1admin user or users used in the existing JP1/Base, you must also confirm that the user is mapped to an OS user with Administrator permissions and that the permission levels shown in the table below are granted.

To create a JP1 user in JP1/Base:

1. Create a JP1 user using JP1/Base, and then set the permission levels as shown in the following table.

Table 1–2: JP1 user permission levels

Permission	JP1 resource group
JP1_AO_Admin	* (Indicates that access to all JP1 resource groups is possible.)
JP1_AJS_Manager	
JP1_JPQ_Admin	

2. Map the created JP1 user to an OS user with Administrator permissions. To map a user other than a built-in administrator who belongs to the Administrator group, disable UAC. If UAC is enabled, an attempt to run a service fails.

> **Tip**
>
> If you edit **Service Share Properties** immediately after installing JP1/AO, you can change the JP1 users who use JP1/AO.

Related topics

- *User Management Setup* in the *Job Management Partner 1/Base User's Guide*
- *List of shared built-in service properties* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- 4.2 Procedure to change a JP1 user

1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2)

To install JP1/AO on a computer that runs Windows Server 2012 or Windows Server 2012 R2, you must first install .NET Framework 3.5.

To install .NET Framework:

1. Start the server manager.
2. Select **Manage**, and then **Add Roles and Features**.
3. Specify `.NET Framework 3.5` and install it.

1.3 New installation of JP1/AO

1.3.1 Procedure to perform a new installation of JP1/AO

You can perform a new installation of JP1/AO from the Hitachi Integrated Installer, as prompted by the wizard.

Before you begin

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

To perform a new installation of JP1/AO:

1. Insert the distribution medium into the drive and run the Hitachi Integrated Installer.

2. Continue the configuration process as prompted by the wizard.
    - Specify the JP1/AO installation folder.
    - Specify the JP1 users to link to JP1/Base and JP1/AJS3.

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
      Setting the backup execution flag and backup folder is required only if the Hitachi Command Suite product is 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 you entered a value other than the default port number, perform the procedure to change the port number.

9. After the installation is complete, execute the `hcmdssrv` command with the `/start` option specified to start the JP1/AO service.

> **Tip**
>
> By specifying JP1 users during installation, you will be able to authenticate users by using JP1/Base functions. JP1 user information that has already been registered can be changed from Service Share Properties in JP1/AO.

Important note

- 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*

- JP1_Automatic Operation is added under **All Programs** in the **Start** menu.
- Some ports used for internal connections in JP1/AO are registered as firewall exceptions.

Related topics

- 1.1 New installation procedure
- 1.2 Pre-installation tasks
- 1.3.2 Installation folder for each product
- 1.3.3 Installation folders for databases
- 1.3.4 Database backup folder
- 4.6.1 Procedure to change the port number used for communications between JP1/AO and Web browsers
- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- *List of shared built-in service properties* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- *Ports used for JP1/AO internal connections* in the *Job Management Partner 1/Automatic Operation Overview and System Design Guide*

1.3.2 Installation folder for each product

The installation folder for each product is specified by using the wizard during installation.

Table 1–4: Default installation folder

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

Item	Installation folder	Modifiable
JP1/Base	*system-drive*\Program Files (x86)\Hitachi\JP1Base#5	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 (x86)\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. Therefore, the *system-drive*`\Program Files (x86)\Hitachi\HiCommand\Base` folder is not created.

#4

The `HiCommand\Base` part is fixed.

If you change the JP1/AO installation folder, it changes the *system-drive*`\Program Files (x86)\Hitachi` path.

#5

The `JP1Base` part is fixed.

The folders shown below cannot be specified as the installation destination. Furthermore, do not specify an installation destination that is under the installation folder for JP1/AO Content Set.

Table 1–5: 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:\`.
Folder for 64-bit applications on a 64-bit version of Windows.	Because this is a 32-bit application, you cannot specify *%programfiles%,%CommonProgramFiles%* or *%WinDir%\system32*.
Network drive	--

Legend:

--: None

Related topics

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

1.3.3 Installation folders for databases

When installing JP1/AO, the wizard lets you specify the installation folder for each product's database.

Table 1–6: Default installation folders for databases

Item	Installation folder	Modifiable
JP1/AO database	*system-drive*\Program Files (x86)\Hitachi\HiCommand \database\Automation#1	Y
Common Component database	*system-drive*\Program Files (x86)\Hitachi\HiCommand \database\BASE#2	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 (x86)\Hitachi\HiCommand\database` path.

Related topics

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

1.3.4 Database backup folder

Backup data is stored in the folder `dbexported_hdb`, which is created in the database backup destination that was specified using the wizard during JP1/AO installation.

Table 1–7: Default backup folder

Item	Backup folder	Modifiable
Database backup data	*system-drive*\Program Files (x86)\Hitachi\Automation_backup \dbexported_hdb#	Y

Legend:

Y: Can be modified.

#

The `dbexported_hdb` part is fixed.

Related topics

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

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

The following table lists the characters that can be specified in the installation, database, and backup folder names.

Table 1–8: 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

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

1.3.6 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 1–9: 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

Item	Character string length	Characters that can be specified (single-byte characters)	Characters that cannot be specified
IPv6 address	47 bytes or less (Including the opening `[` and closing `]`)	A-F a-f 0-9 . : [ ]	- `]` 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 1–10: Manuals and the folders to create for them

Manual	Folder to be created
Job Management Partner 1/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
Job Management Partner 1/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
Job Management Partner 1/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
Job Management Partner 1/Automatic Operation GUI, Command, and API Reference	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOGR English environment: *JP1/AO-installation-folder*\docroot\help\en\AOGR Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOGR
Job Management Partner 1/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
Job Management Partner 1/Automatic Operation Messages	Japanese environment: *JP1/AO-installation-folder*\docroot\help\ja\AOMR

Manual	Folder to be created
Job Management Partner 1/Automatic Operation Messages	English environment: *JP1/AO-installation-folder*\docroot\help\en\AOMR Chinese environment: *JP1/AO-installation-folder*\docroot\help\zh\AOMR
Job Management Partner 1/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

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

   Files to be copied

   All HTML files and GRAPHICS folders under *drive-in-which-manual-distribution-medium-is-inserted*\MAN \3021\0*number-based-on-manual-number*#D

   # This number omits the first four digits of the manual's document number and the hyphen (-). If the number is less than six digits, 00 is added to the end.

   Destination folders

   Folders that you created in step 2

   For details about the relationship between manual names and document numbers, see *Reference material for this manual* in the *Job Management Partner 1/Automatic Operation Overview and System Design Guide*.

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

   Japanese environment:

   JP1/AO-installation-folder\docroot\help\ja\INDEX.HTM

   English environment:

   JP1/AO-installation-folder\docroot\help\en\INDEX.HTM

   Chinese environment:

   JP1/AO-installation-folder\docroot\help\zh\INDEX.HTM

5. Copy the file shown below.

   Japanese environment:

   File to be copied

   JP1/AO-installation-folder\docroot\help\INDEX_JA.HTM

   Destination folder

   JP1/AO-installation-folder\docroot\help\ja

   English environment:

   File to be copied

   JP1/AO-installation-folder\docroot\help\INDEX_EN.HTM

   Destination folder

   JP1/AO-installation-folder\docroot\help\en

   Chinese environment:

File to be copied

JP1/AO-installation-folder\docroot\help\INDEX_ZH.HTM

Destination folder

JP1/AO-installation-folder\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
- 1.3.2 Installation folder for each product

1.5 Installing JP1/AO Content Set

1.5.1 Procedure to install JP1/AO Content Set

When you install JP1/AO Content Set, you will be able to use service templates or Service Template Set in JP1/AO. JP1/AO Content Set is installed from the Hitachi Integrated Installer, as prompted by the wizard.

Before you begin

- Log in to the server as a user with Administrator permissions.
- Confirm that JP1/AO is installed.

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

To install JP1/AO Content Set:

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

   Do not install JP1/AO Content Set 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.

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 Set

  Version:

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

  JP1/AO-Content-Set-installation-folder\contents\setup

  You can use the**Add Service** dialog box or the `listservices` command to confirm that the service templates have been imported.

Related topics

- 1.5.2 JP1/AO Content Set installation folder

1.5.2 JP1/AO Content Set installation folder

The installation folder for JP1/AO Content Set is specified by using the wizard during installation.

Do not install JP1/AO Content Set in the same installation folder as JP1/AO.

Table 1–11: Default installation folder for JP1/AO Content Set

Item	Character string length	Installation folder	Modifiable
JP1/AO Content Set	150 bytes or less	*system-drive*\Program Files (x86)\Hitachi\JP1AOCONTSET#	Y

Legend:

Y: Can be modified.

#

The `JP1AOCONTSET` part is fixed.

Related topics

- 1.5.1 Procedure to install JP1/AO Content Set

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 permissions.

To acquire an SSL server certificate:

1. Execute the `hcmdsssltool` command in the command prompt 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

Set up the 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 permissions.
- Stop the JP1/AO service.

  For non-cluster systems:

  Execute the `hcmdssrv` 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 httpsd.conf file so that HTTPS connections can be used.

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

Common-Component-installation-folder\httpsd\conf

In the httpsd.conf file, the directives to use HTTPS connections are commented out by default, and use of HTTP connections is specified. To enable HTTPS connections, change the httpsd.conf file as follows:

- Comment out the directives that are not necessary for HTTPS connections.
- Add the directives necessary for HTTPS connections.
- Enable the directives that are necessary for HTTPS connections and that are commented out by default.

> **Tip**
>
> In the httpsd.conf file, lines that begin with a hash mark (#) are treated as comment lines. Deleting # at the beginning of a line allows the line to function as a directive.

The following shows the settings in the httpsd.conf file after JP1/AO is installed (HTTP connections are used), and the settings in the httpsd.conf file that are changed to use HTTPS connections. In the following example, default port numbers are used: 23015 for HTTP connections and 23016 for HTTPS connections.

Settings of the httpsd.conf file for using HTTP connections (default)

```
Listen 23015
Listen [::]:23015
SSLDisable

SSLSessionCacheSize 0
#Listen 23016
#Listen [::]:23016
#<VirtualHost *:23016>
#  ServerName JP1/AO-server-name-or-IP-address
#  SSLEnable
#  SSLProtocol SSLv3 TLSv1
#  SSLRequiredCiphers AES256-SHA:AES128-SHA:DES-CBC3-SHA
#  SSLRequireSSL
#  SSLCertificateFile "Common-Component-installation-folder/httpsd/
conf/ssl/server/httpsd.pem"
#  SSLCertificateKeyFile "Common-Component-installation-folder/httpsd/
conf/ssl/server/httpsdkey.pem"
#  SSLCACertificateFile "Common-Component-installation-folder/httpsd/
conf/ssl/cacert/anycert.pem"
#  SSLSessionCacheTimeout 3600
#</VirtualHost>
```

Settings of the httpsd.conf file for using HTTPS connection (after the change)

```
#Listen 23015#1
#Listen [::]:23015#1
Listen 127.0.0.1:23015#2
SSLDisable

SSLSessionCacheSize 0
Listen 23016#3
Listen [::]:23016#3
<VirtualHost *:23016>#3
  ServerName JP1/AO-server-name-or-IP-address#3
  SSLEnable#3
  SSLProtocol SSLv3 TLSv1#3#4
  SSLRequiredCiphers AES256-SHA:AES128-SHA:DES-CBC3-SHA#3
  SSLRequireSSL#3
  SSLCertificateFile "Common-Component-installation-folder/httpsd/
conf/ssl/server/httpsd.pem"#3
  SSLCertificateKeyFile "Common-Component-installation-folder/httpsd/
conf/ssl/server/httpsdkey.pem"#3
#  SSLCACertificateFile "Common-Component-installation-folder/httpsd/
conf/ssl/cacert/anycert.pem"#5
  SSLSessionCacheTimeout 3600#3
</VirtualHost>#3
```

#1

This directive is not necessary for using HTTPS connections. Add # at the beginning of the line to comment out the line.

#2

Add this line as a directive necessary for using HTTPS connections.

#3

This directive is necessary for using HTTPS connections. Delete # at the beginning of the line to enable the line.

#4

Specify "TLSv11 TLSv12" for the SSLProtocol. By doing so, you can allow connections using only TLS 1.1 or TLS 1.2.

#5

This directive is necessary for using the SSL server certificate issued by the chained CA for using HTTPS connections. If necessary, delete # at the beginning of the line to enable the line.

> **Tip**
>
> The SSL server certificate file and private key file can be stored not only in the *Common-Component-installation-folder*, but also in any folder specified in the httpsd.conf file. Do not include junctions or symbolic links in the specified folder.

2. For the SSLCertificateFile directive, specify the location of the SSL server certificate file by using an absolute path.
   Store the SSL server certificate file in the path specified by the SSLCertificateFile directive in the httpsd.conf file.
3. For the SSLCertificateKeyFile directive, specify the location of the private key file by using an absolute path.
   Store the private key file in the path specified by the SSLCertificateKeyFiled directive in the httpsd.conf file.
4. If you want to use the SSL server certificate file issued by the chained CA, use the SSLCACertificateFile directive to specify the location of the chained CA certificate file by using an absolute path.
5. Execute the `hcmdsfwcancel` command to register firewall exceptions.
6. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` command with the `/start` option specified.

   For cluster systems:

   Use the cluster software to bring the service online.
7. Update the URL information used for establishing a connection from the Web browser to the JP1/AO server.

   Execute the `hcmdschgurl` 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.

Related topics

- *Starting and stopping JP1/Base* in the *Job Management Partner 1/Base User's Guide*
- *Logging in to JP1/AO* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- *Maintenance* in the *Job Management Partner 1/Automatic Operation Administration Guide*

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 or public key 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.

Related topics

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

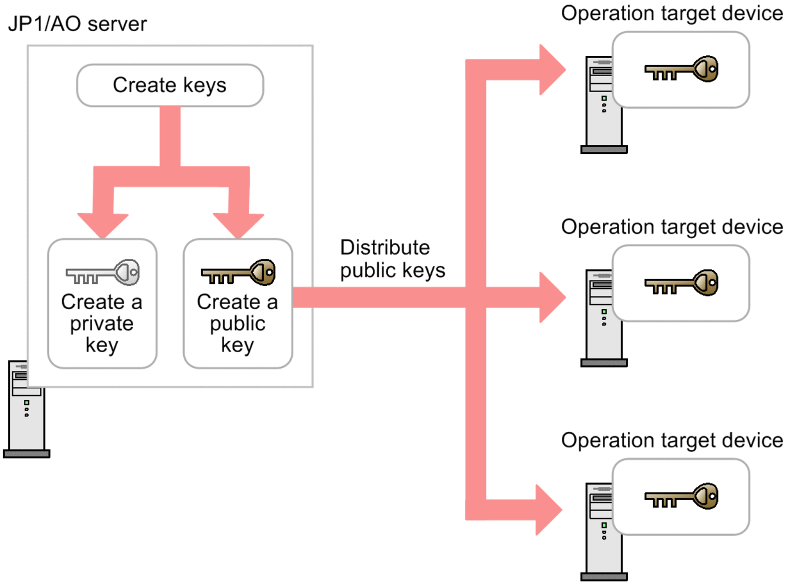
1.7.2 Public key authentication available for JP1/AO

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)

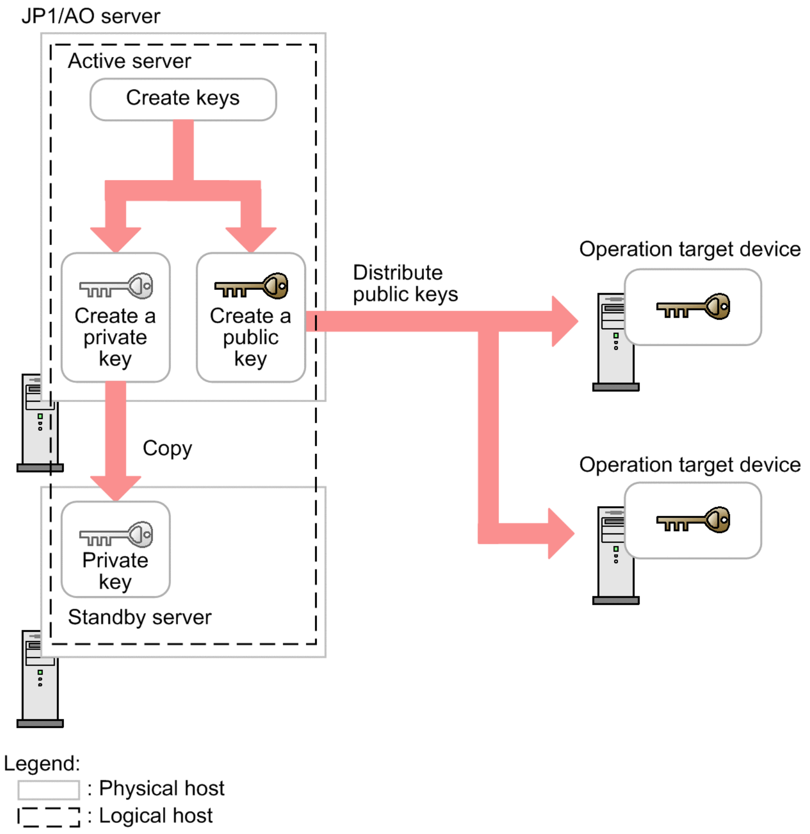
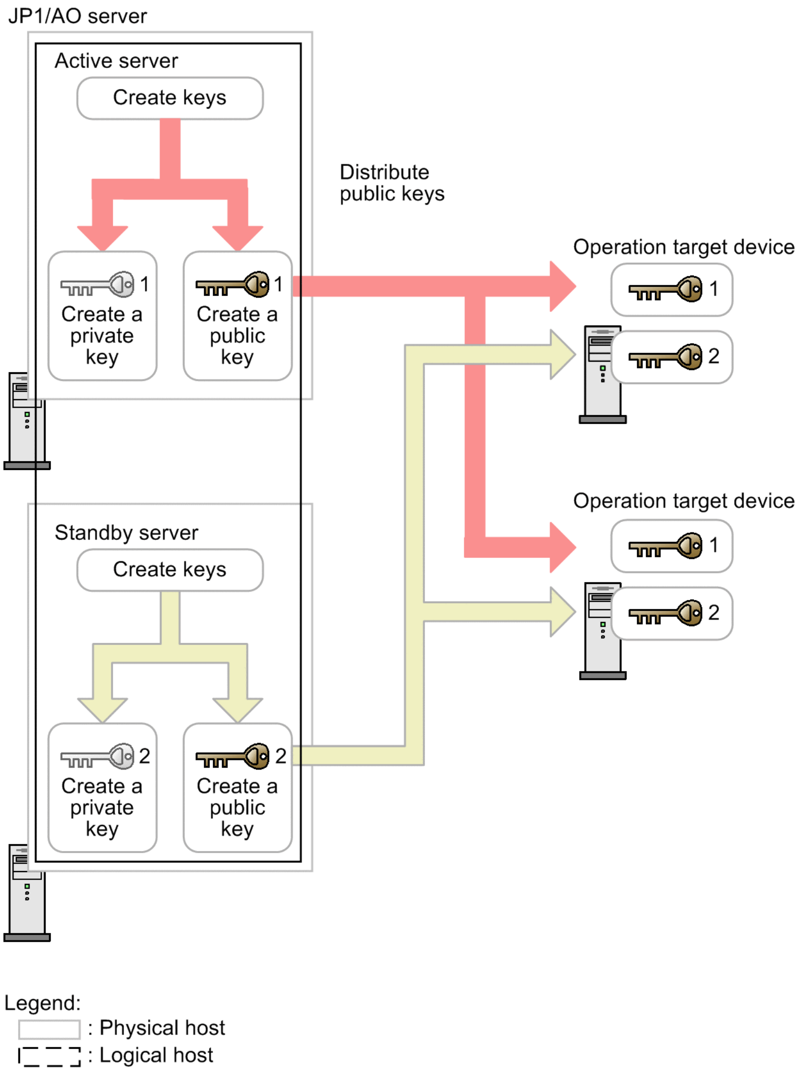


Figure 1–3: Deployment of keys for public key authentication (using different keys for the active server and the standby server)



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 Linux (example of Red Hat Enterprise Linux 6.4):
     `/etc/rc.d/init.d/sshd restart`
   - In Solaris (Solaris 10)
     `/usr/sbin/svcadm restart ssh`
   - In AIX (AIX 6.1):
     `kill -HUP` *`sshd-process-ID`*
   - In HP-UX (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 depends on the OS. Create the public key file and private key file according to the OS specifications of the operation target device.

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. Use an absolute path to specify the private key file for ssh.privateKeyFile in the property file (config_user.properties).

> **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 **Service Share Properties** view, select the **Pass phrase of the private key (for SSH public key authentication)** shared built-in service property, and then click the **Set Service Share Property** button.

2. In the **Set Service Share Property** dialog box, in the **Value** text box, enter the passphrase 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 Property file (config_user.properties)
- *List of shared built-in service properties* in the *Job Management Partner 1/Automatic Operation Administration Guide*

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	Property file (config_user.properties)	2.2 Property 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 disabling the Authenticode signing function	OS configuration file	2.9 Settings in an environment where external networks cannot be connected

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.

2.2 Property 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

For cluster systems:

shared-folder-name\jp1ao\conf

Trigger for applying definitions

Restarting the service (HAutomation Engine Web Service)

Description

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

Classification	Key name	Settings	Specifiable values	Default value
Logs[#1]	logger.sysloglevel	Specifies the threshold for event log output.	• 0: Messages whose output level is 0 are output. • 10: Messages whose output level is 0 and 10 are output.	0
	logger.message.server.MaxBackupIndex	Specifies the maximum number of log backup files for a server.	1-16	7
	logger.message.server.MaxFileSize	Specifies the maximum log file size (KB) for a server.	4-2,097,151	1,024
	logger.message.command.MaxBackupIndex	Specifies the maximum number of log backup files for a command.	1-16	7

Classification	Key name	Settings	Specifiable values	Default value
Logs[#1]	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	1,0240
Task management	task.ajs.IPBindhost	Specifies the JP1/AO host name or IP address (0-255 bytes) when the JP1/Base communication protocol is set to the IP binding method.	Character string that can be specified for host names or IP addresses	" " (null character)
	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.details.jobnet.status.visible	Specifies whether the step list in the **Task Details** dialog box displays the status in the task-processing engine or the status of steps.	• true: Display the status in the task-processing engine • false: Display the status of steps	false
Service management	packagemanager.extraPresets.maxFiles	Specifies the maximum number of preset property definition files that can be added to one service template.	5-100	5
JP1 event notifications	notification.jp1event	Specifies whether to send JP1 events in the notification function.	• true: Send • false: Do not send	true
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

Classification	Key name	Settings	Specifiable values	Default value
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
	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	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 in advance. 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	If the OS of the operation target device is UNIX, this property specifies the path to the execution directory used to execute a	Character string of 0-128 characters	" " (null character)

Classification	Key name	Settings	Specifiable values	Default value
Remote command	plugin.remoteCommand.executionDirectory.ssh	content plug-in. Note that the execution directory must be created in advance.	Character string of 0-128 characters	" " (null character)
	plugin.remoteCommand.workDirectory.ssh[#2]	If the OS of the operation target device is UNIX, this property specifies a work folder [#3] used to execute file-forwarding 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.	Single-byte alphanumeric characters, and the following symbols: / (used as a path separator), -, _, .	/tmp/Hitachi_AO
Retry remote host connection	ssh.connect.retry.times	Specifies the number of retries, in the event of a failed SSH connection to the operation target device.	0-100	3
	ssh.connect.retry.interval	Specifies the interval (seconds) between retries, in the event of a failed SSH connection to the operation target device.	1-600	10
	wmi.connect.retry.times	Specifies the number of retries, in the event of a failed WMI connection to the operation target device.	0-100	3
	wmi.connect.retry.interval	Specifies the interval (seconds) between retries, in the event of a failed WMI 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 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-forwarding 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

Classification	Key name	Settings	Specifiable values	Default value
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: !, #, $, &, (,), +, ,, -, ., ;, =, @, [,], ?, _, `, {, }, ~	*JP1/AO-installation-folder*\logs[#4]
	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[#5]	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 Windows user ID to the subject identification information.	false
Window refresh	client.events.refreshinterval	Specifies the refresh interval (seconds) for events.	0-65,535	5
Link&Launch function	linkandlaunch.hcs.enabled	Specifies whether to display links to the Hitachi Command Suite products in the **Tools** menu.	• true: Display links. • false: Do not display links.	false
Editor	client.editor.upload.maxfilesize	Specifies the maximum file size (MB) that can be specified when a file is uploaded by using the **Editor** window. The file size can be specified for each of the following files: • Plug-in icon file • Script file executed by a plug-in • Plug-in resource file • Service resource file • Window custom file	1-10	3

Classification	Key name	Settings	Specifiable values	Default value
Editor	server.editor.step.perTemplate.maxnum#6	Specifies the maximum number of steps per service template.	320-40,000 #7	320
	server.editor.step.perLayer.maxnum#6	Specifies the maximum number of steps per layer.	80-10,000 #7	80
	client.editor.canvas.maxwidth#6	Specifies the maximum width (unit: px) of the operational region in the **Flow** view. 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#6	Specifies the maximum height (unit: px) of the operational region in the **Flow** view. The estimate expression is as follows: Height (px) = number-of-steps-to-be-deployed-vertically x 300 (px)	2,400-30,000	2,400
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
Task monitor	client.monitor.tasklog.maxfilesize	Specifies the size of task logs (KB) displayed in the **Task Log** dialog box.	4-10,240	1,024
	client.monitor.tasklog.refresh.interval	Specifies the automatic refresh interval (seconds) of the **Task Log** dialog box.	30-300	30
	client.monitor.status.interval	Specifies the automatic refresh interval (seconds) of the task monitor.	30-300	30

#1

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

#2

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

#3

- The work folder must have read, write, and execution permissions for the connected user.
- If the path specified for the work folder does not exist when a file-forwarding plug-in or content plug-in is executed, a work folder is created during execution of the plug-in. The created work folder is assigned access

permission 777 (that is, access permission is given to all users). If an attempt to create the work folder fails, execution of the plug-in terminates abnormally.

#4

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

#5

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

#6

These properties are defined to provide compatibility with JP1/AO 10-00.

#7

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 10-00.
- The total number of steps in the service template to be edited exceeds 320, or the number of steps per layer exceeds 80.

Example definitions

```
logger.sysloglevel = 0
logger.message.server.MaxBackupIndex = 7
logger.message.server.MaxFileSize = 1024
logger.message.command.MaxBackupIndex = 7
logger.message.command.MaxFileSize = 1024
logger.TA.MaxFileSize = 10240
task.ajs.IPBindhost =
tasklist.autoarchive.taskRemainingPeriod = 7
tasklist.autoarchive.executeTime = 04:00:00
tasklist.autoarchive.maxTasks = 5000
tasklist.autodelete.maxHistories = 30000
task.details.jobnet.status.visible = false
packagemanager.extraPresets.maxFiles = 5
plugin.remoteCommand.workDirectory.ssh = /tmp/Hitachi_AO
notification.jp1event = true
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.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
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 (x86)\\Hitachi\\JP1AO\\logs
logger.Audit.MaxBackupIndex = 7
logger.Audit.MaxFileSize = 1024
logger.Audit.command.useLoginUserID = false
client.events.refreshinterval = 5
linkandlaunch.hcs.enabled = false
client.editor.upload.maxfilesize = 3
server.editor.step.perTemplate.maxnum = 320
server.editor.step.perLayer.maxnum = 80
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
client.monitor.tasklog.maxfilesize = 1024
client.monitor.tasklog.refresh.interval = 30
client.monitor.status.interval = 30
```

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

For cluster systems:
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	23015

Example definitions

```
command.http.port = 23015
```

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/mailDefinition">
<title>email-title</title>
<body>email-body</body>
</mail>
```

Installation folder

For non-cluster systems:
JP1/AO-installation-folder\conf

For cluster systems:
shared-folder-name\jp1ao\conf

Trigger for applying definitions

Starting 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。	リソースグループ名:$RESOURCE_GROUP_NAME$ 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 $TASK_STATUS$	Resource 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。	资源群组名:$RESOURCE_GROUP_NAME$ 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;
<	&lt;
>	&gt;
"	&quot;
'	&apos;

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
$RESOURCE_ GROUP_NAME$	Resource group name	Set to the character string representing the resource group name.
$TASK_NAME$	Task name	Set according to the format in the task properties.
$TASK_ID$	Task ID	
$TASK_KIND$	Task type	
$SERVICE_NAME$	Service name	
$SERVICE_CATEGORY$	Service category	
$TASK_STATUS$	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 resource 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/mailDefinition">
<title>[Automatic Operation]$TASK_NAME$ has changed to $TASK_STATUS$</
title>
<body>
Resource Group Name:$RESOURCE_GROUP_NAME$
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

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-forwarding 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

For cluster systems:
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

Key name	Settings	Specifiable values
terminal.charset	Specifies the character set used for communication.	- 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 property 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-forwarding plug-in - Terminal connect plug-in - Content plug-in This setting has priority over the ssh.port.number setting in the property 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 (,)

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

For cluster systems:

shared-folder-name\jp1ao\conf\plugin

Trigger for applying definitions

Starting 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

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
	auth.server.name	Specifies the server identifier of the external authentication server to be linked. You can use a maximum of 64 bytes.	• ASCII printable character code (0x21-7E) excluding the	-- (Initial value at installation: ServerName)

Classification	Key name	Settings	Specifiable values	Default values
Common item	auth.server.name	You must specify this property if `ldap` is specified for `auth.server.type`. For other cases, there is no need to specify this property.	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	Specify `ldap`. There is no need to specify this property if a value other than `ldap` is specified for `auth.server.type`.	ldap	--
	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.	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
	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 in an environment where external networks cannot be connected

JP1/AO uses Authenticode signed programs, which connect to an external network as needed to check signatures. Therefore, several tens of seconds might be required to execute a plug-in that works as an extension of a service in an environment where external networks cannot be connected.

To use JP1/AO in an environment where external networks cannot be connected, specify the following settings on the JP1/AO server to disable the Authenticode signature function and reduce the time required to execute a plug-in:

1. Use a text editor to open the following files:
   system-drive:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet.config
   system-drive:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
2. Specify `false` for `generatePublisherEvidence enabled` as shown below, and then save the files.

```
<configuration>
<runtime>
<generatePublisherEvidence enabled="false"/>
</runtime>
</configuration>
```

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 `hcmdscheckauth` command.	Required	3.1.5 Procedure to check the link to JP1/Base

Related topics

- *Linking with JP1/Base authentication* in the *Job Management Partner 1/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

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 resource group name.
   If you want to grant All Resources permission, specify an asterisk (*) for the JP1 resource group name.

Related topics

- *User Management Setup* in the *Job Management Partner 1/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 Resources`.

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
system-drive\Program Files (x86)\Hitachi \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 *Job Management Partner 1/Base User's Guide*
- *Evaluating users and access permissions* in the *Job Management Partner 1/Automatic Operation Overview and System Design Guide*
- *jbsaclreload* in the *Job Management Partner 1/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 `hcmdscheckauth` command.

Related topics

- *hcmdscheckauth (verifying the connection with the external authentication server)* in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*

3.2 Linking with Active Directory

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#	Optional#	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	Execute the `hcmdscheckauth` 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
5	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
6	Assign roles to Active Directory groups.	Not required	Required	3.2.7 Assigning roles to Active Directory groups

#

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

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 *Job Management Partner 1/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

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 (fixed)	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
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.

#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.

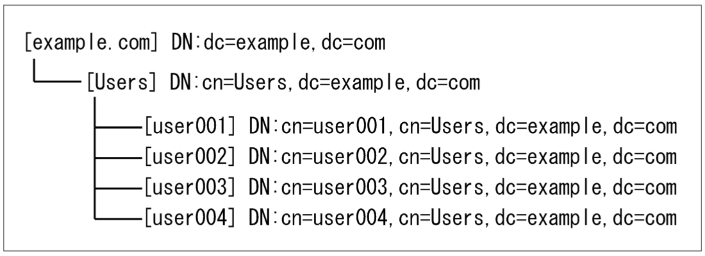
LDAP search information includes:

- 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.

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.

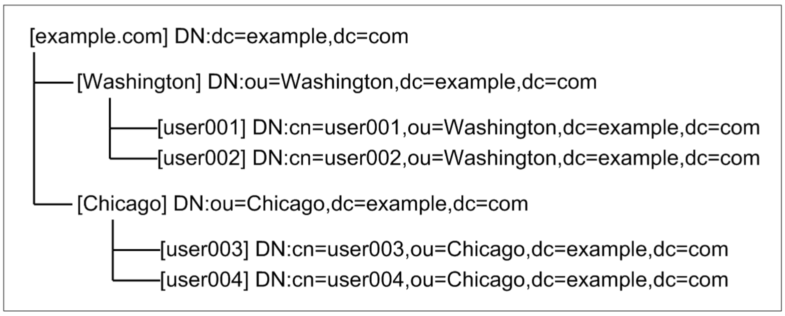
      Figure 3–1: Example of DIT structure (if there is no need to register LDAP search users)

```
[example.com] DN:dc=example,dc=com
└──[Users] DN:cn=Users,dc=example,dc=com
        ├──[user001] DN:cn=user001,cn=Users,dc=example,dc=com
        ├──[user002] DN:cn=user002,cn=Users,dc=example,dc=com
        ├──[user003] DN:cn=user003,cn=Users,dc=example,dc=com
        └──[user004] DN:cn=user004,cn=Users,dc=example,dc=com
```

      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.
      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)


[example.com] DN:dc=example,dc=com
[Washington] DN:ou=Washington,dc=example,dc=com
[user001] DN:cn=user001,ou=Washington,dc=example,dc=com
[user002] DN:cn=user002,ou=Washington,dc=example,dc=com
[Chicago] DN:ou=Chicago,dc=example,dc=com
[user003] DN:cn=user003,ou=Chicago,dc=example,dc=com
[user004] DN:cn=user004,ou=Chicago,dc=example,dc=com

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 `hcmdsldapuser` 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

- *hcmdsldapuser* in the manual *Job Management Partner 1/Automatic Operation GUI, 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 `hcmdscheckauth` 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

hcmdscheckauth in the manual *Job Management Partner 1/Automatic Operation GUI, 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

- *Registering users in JP1/AO* in the *Job Management Partner 1/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 resource groups and roles to the registered user groups.

Related topics

- *Registering Active Directory groups linking with JP1/AO* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- *Assigning resource groups and roles to user groups* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.3 Linking to Hitachi Command Suite products

3.3.1 Procedure to enable single sign-on to Hitachi Command Suite products

To enable single sign-on to Hitachi Command Suite products by using the Link & Launch feature, you must define the permission levels and edit the properties file.

Before you begin

- Confirm that the Hitachi Command Suite products to be launched have been installed on the JP1/AO server.
- The URL to be launched uses the host name or IP address specified during the installation of the Hitachi Command Suite products. Therefore, make sure that the host name resolves correctly on the terminal on which you want to use JP1/AO from the Web browser.
- If you want to allow JP1 users to use single sign-on to Hitachi Command Suite products, make sure that they are linked to the JP1/Base authentication function.

To enable single sign-on to Hitachi Command Suite products:

1. If you want to allow JP1 users to use single sign-on to Hitachi Command Suite products, define permission levels in JP1/Base.

2. In the property file (config_user.properties), specify `true` for the linkandlaunch.hcs.enabled key.

3. In the **Tasks** window, check the tasks. If any tasks are in the execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), stop execution of the tasks or wait until the task status changes to the ended status.

4. Stop the JP1/AO service.

   For non-cluster systems:

      Execute the `hcmdssrv` command with the `/stop` option specified.

   For cluster systems:

      Use the cluster software to bring the service offline.

5. Start the JP1/AO service.

   For non-cluster systems:

      Execute the `hcmdssrv` command with the `/start` option specified.

   For cluster systems:

      Use the cluster software to bring the service online.

Results of procedure

Single sign-on to all Hitachi Command Suite products is enabled, and links to the products appear in the **Tools** menu.

Related topics

- 3.1 Linking to the JP1/Base authentication function
- 3.3.2 Defining permissions in JP1/Base (for single sign-on to all Hitachi Command Suite products)
- 2.2 Property file (config_user.properties)

- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.3.2 Defining permissions in JP1/Base (for single sign-on to all Hitachi Command Suite products)

To allow users managed by JP1/Base to use a single sign-on from JP1/AO to Hitachi Command Suite products, you must set permission levels in JP1/Base for each product.

Table 3–8: Defining permissions in JP1/Base (for single sign-on to Hitachi Command Suite products)

Product name	Role or authority in product	Permission level to set in JP1/Base
Common Component	User Management	HCS_UserMng_Admin
Device Manager	Admin	HCS_HDvM_Admin
	StorageAdmin	HCS_HDvM_Storage
	Guest	HCS_HDvM_Guest
	Peer	HCS_HDvM_Peer
Replication Manager	Admin	HCS_HRpM_Admin
	Modify	HCS_HRpM_Modify
	View	HCS_HRpM_View
Tiered Storage Manager	Admin	HCS_HTSM_Admin
	Execute	HCS_HTSM_Execute
	Modify	HCS_HTSM_Modify
	View	HCS_HTSM_View
Storage Navigator Modular	Modify	HCS_HSNM2_Modify
	View	HCS_HSNM2_View
File Services Manager	Admin	HCS_HFSM_Admin
Compute Systems Manager	Admin	HCS_HCSM_Admin
	Modify	HCS_HCSM_Modify
	View	HCS_HCSM_View
Global Link Availability Manager	Admin	HCS_HGLM_Admin
	Modify	HCS_HGLM_Modify
	View	HCS_HGLM_View
Tuning Manager	Admin	HCS_HTnM_Admin
	View	HCS_HTnM_View

Related topics

- *User Management Setup* in the *Job Management Partner 1/Base User's Guide*

3.4 Linking to the JP1/IM event monitoring function

3.4.1 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.

   If the OS is different between the source and destination of the copied definition files, conversion of the file's character encoding might be required. To copy the definition files from JP1/AO in a Windows environment to JP1/IM in a Linux environment, you must first convert the character encoding to UTF-8 by using a text editor, the `nkf` command, or some other 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 property 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 *Job Management Partner 1/Automatic Operation Overview and System Design Guide*
- 3.4.2 Definition files used for linking to JP1/IM
- 3.4.3 Integrated function menu definition file (hitachi_jp1_ao_tree.conf)
- 3.4.4 Target folders into which definition files for linking to JP1/IM (in a Windows environment) are copied
- 3.4.5 Target directories into which definition files for linking to JP1/IM (for a UNIX environment) are copied
- 2.2 Property file (config_user.properties)

3.4.2 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

For non-cluster systems:

JP/AO-installation-folder\conf\event

For cluster systems:

shared-folder-name\jp1ao\conf\event

Table 3–9: 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. The definition files have the same name.

Related topics

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

3.4.3 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:
JP/AO-installation-folder\conf\event\jp1imview\ja

English environment:
\JP/AO-installation-folderconf\event\jp1imview\en

Chinese environment:
JP/AO-installation-folder\conf\event\jp1imview\zh

For cluster systems:

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

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

Chinese environment:
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 23015:

```
#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:23015/Automation/launcher/Login?jp1token=
%JCO_JP1TOKEN$ENC$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:23015/Automation/launcher/Login?jp1token=
%JCO_JP1TOKEN$ENC$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:23015/Automation/launcher/Login?jp1token=
%JCO_JP1TOKEN$ENC$URLENC%";
@define-block-end;
```

Related topics

- 3.4.1 Procedure for linking to the JP1/IM event monitoring function
- *Evaluating the system configuration* in the *Job Management Partner 1/Automatic Operation Overview and System Design Guide*

3.4.4 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 3–10: 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

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

3.4.5 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 3–11: 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

Definition file	Directory to copy it to
Definition file for object types	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

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

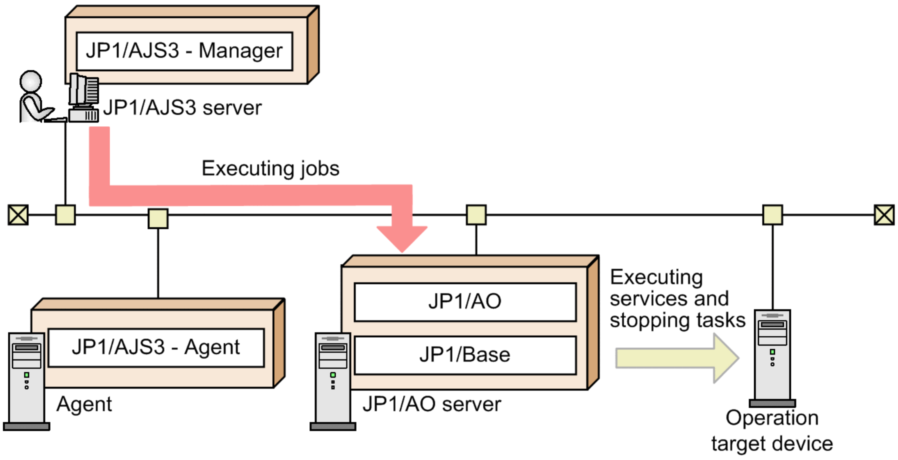
3.5 Linking to JP1/AJS3

3.5.1 Procedure for linking to JP1/AJS3

By linking to JP1/AJS3, you will be able to automatically execute the following commands on the JP1/AO server from the JP1/AJS3 server:

- `stoptask` command
- `submittask` command

Figure 3–3: Liking to JP1/AJS3



Before you begin

If the firewall is enabled on the JP1/AO server, exceptions must be registered in the firewall. Register the following ports, which are used for communication with JP1/AJS3 - Manager, as exceptions in the firewall settings for the JP1/AO server.

- 20241/tcp (jp1ajs2qman)
- 20242/tcp (jp1ajs2qagt)
- 20243/tcp (jp1ajs2qnfy)

To link to JP1/AJS3:

1. Execute the `ajsagtadd` command for JP1/AJS3 - Manager on the JP1/AJS3 server to register JP1/AO as an execution agent.
   In the `ajsagtadd` command, specify any name for the `-a` option, and specify the name of the JP1/AO server for the `-s` option.

2. Define the PC job in the jobnet definition of the JP1/AJS3 server.
   In the **Define Details - [PC Job]** dialog box, specify as follows:
   - For **Exec-agent**, specify the name you specified for the `-a` option in step 1.
   - On the **Definition** page, for **File name**, specify the name of the file for the `stoptask` or `submittask` command.
   - On the **Definition** page, for **Parameters**, specify the arguments to be specified for the command.

- On the **Attributes** page, for **Exec. Service**, specify **Standard**.

3. Register the jobnet that contains the PC job you defined in step 2 for execution on the JP1/AJS3 server.

Remarks

- The maximum number of tasks (including debug tasks) that can be managed on a JP1/AO server can be defined in the property file (config_user.properties). The default value is 5,000. Make sure that the sum of the number of tasks generated by using any of the methods listed below does not exceed the value specified in the property file (config_user.properties). If the number of tasks exceeds the maximum, excess tasks are automatically archived and excess debug tasks are automatically deleted, beginning from the task or debug task with the oldest stop date and time.
  - Tasks generated by executing a service in the **Submit Service** dialog box
  - Debug tasks generated by debugging
  - Tasks generated by executing the `submittask` command on the JP1/AO server
  - Tasks generated by executing the `submittask` command from the JP1/AJS3 server

Related topics

- *stoptask* and *submittask* in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*
- *ajsagtadd* in the manual *Job Management Partner 1/Automatic Job Management System 3 Command Reference*
- *Define Details - [PC Job] dialog box* in the *Job Management Partner 1/Automatic Job Management System 3 Operator's Guide*

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 you change the installation folder, the definitions in the property file (config_user.properties) cannot be recovered from a backup. After reinstalling JP1/AO, re-set the definitions.

Related topics

- 1.3.2 Installation folder for each product
- 8.1 Uninstallation procedure
- 1.1 New installation procedure
- 2.2 Property file (config_user.properties)

4.2 Procedure to change a JP1 user

You can use the JP1/AO window to change JP1 users so that they can connect to JP1/AJS3.

Before you begin

Confirm that no tasks are running in JP1/AO.

To change a JP1 user:

1. Select **Service Share Properties** in the left pane of the **Administration** window.
2. Select **JP1 user name** from the right pane and click the **Set Service Share Property** button.
3. Enter the new JP1 user name and click the **OK** button.
4. Select **JP1 user password** from the right pane and click the **Set Service Share Property** button.
5. Enter the new JP1 user password and click the **OK** button.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base

4.3 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 you change the database installation folder, the definitions in the property file (config_user.properties) cannot be recovered from a backup. After reinstalling JP1/AO, re-set the definitions.

Related topics

- 1.3.3 Installation folders for databases
- 8.1 Uninstallation procedure
- 1.1 New installation procedure
- 2.2 Property file (config_user.properties)

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

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

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

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

Table 4–1: Procedure to change the host name of the JP1/AO server

Task		Reference
1	Perform a backup of JP1/AO.	*Backing up data in a JP1/AO system (non-cluster configuration)* in the *Job Management Partner 1/Automatic Operation Administration Guide* However, the backup procedure for JP1/Base described in that section is not necessary.
2	Change the host name of the JP1/AO server.	--
3	Restart the JP1/AO server.	--
4	In JP1/Base, perform the steps required for changing the host name.	*Effects and follow-up tasks when changing host names* in the *Job Management Partner 1/Base User's Guide*
5	Perform a restore of JP1/AO.	*Restoring data in a JP1/AO system (non-cluster configuration)* in the *Job Management Partner 1/Automatic Operation Administration Guide* However, the restore procedure for JP1/Base described in that section is not necessary.
6	Start the JP1/Base service.	*Startup and Termination* in the *Job Management Partner 1/Base User's Guide*
7	Execute the `hcmdssrv` command with the `/start` option specified to start the JP1/AO service.	--
8	Execute the following commands in the command prompt: • `set JP1_USERNAME=`*JP1-user-name-specified-during-installation* • `ajsagtalt -a loop -s` *new-host-name*# • `ajsagtalt -a userResponse -s` *new-host-name*#	--
9	Execute the `hcmdschgurl` command to update the URL.	4.7 Procedure to change the URL

Legend:

--: None

#

Commands whose name begins with `ajs` are contained in the folder for task-processing engine system files. For details, see A.1 List of folders.

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

To change the host name, you must uninstall JP1/AO, and then re-install it.

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

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

Before you begin

Log in to the JP1/AO server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

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

Table 4–2: Procedure to change the host name of the JP1/AO server

Task		Reference
1	Perform a backup	*Backing up data in a JP1/AO system (cluster configuration)* in the *Job Management Partner 1/Automatic Operation Administration Guide* However, the backup procedure for JP1/Base described in that section is not necessary.
2	Uninstall JP1/AO.	8.1 Uninstallation procedure
3	Change the logical host name of the JP1/AO server.	--
4	In JP1/Base, perform the steps required when changing the host name.	*Effects and follow-up tasks when changing host names* in the *Job Management Partner 1/Base User's Guide*
5	Install JP1/AO and set up the cluster environment.	5. Setting up a cluster system
6	Perform a restore of the active server.	*Restoring data in a JP1/AO system (cluster configuration)* in the *Job Management Partner 1/Automatic Operation Administration Guide* However, the restore procedure for JP1/Base described in that section is not necessary.
7	Bring online the following script and services, which are registered in the cluster software: • `stopcluster` command • HAutomation Engine *logical-host-name* • HAutomation Engine Web Service • HBase Storage Mgmt Web Service • HBase Storage Mgmt Common Service • HiRDB/ClusterService _HD0 • JP1/Base_*logical-host-name* • JP1/Base Event *logical-host-name*	--
8	Execute the following commands in the command prompt on the active server: • `set JP1_USERNAME=`*JP1-user-name-specified-during-installation* • `ajsagtalt -a loop -s` *`logical-host-name`* `-h` *`logical-host-name`*# • `ajsagtalt -a userResponse -s` *`logical-host-name`* `-h` *`logical-host-name`*#	--

Task		Reference
9	Execute the`hcmdschgurl` command to update the URL.	4.7 Procedure to change the URL

Legend:

--: None

#

Commands whose name begins with `ajs` are contained in the folder for the task-processing engine system files. For details, see A.1 List of folders.

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

4.5.1 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 and JP1/Base services.

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 Response, Abnormal Detection, or Terminated), stop execution of the tasks or wait until the task status changes to the ended status.

2. Execute the `hcmdssrv` command with the `/stop` option specified to stop the JP1/AO service.

3. Stop the JP1/Base service.

4. Change the IP address of the JP1/AO server.

5. Execute the `hcmdssrv` command with the `/start` option specified to start the JP1/AO service.

Related topics

- *Startup and Termination* in the *Job Management Partner 1/Base User's Guide*

4.5.2 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 domain user with Administrator permissions on the OS and 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 the execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), 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.

4.6 Procedure to change the port number

4.6.1 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 the execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), 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:

1. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` command with `/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:
   The settings to be changed depend on the communication protocol between the JP1/AO and the Web browser.

   If the communication protocol is HTTP:

   - `Listen` in *Common-Component-installation-folder*\httpsd\conf\httpsd.conf

     Specify the new number in the place of 23015 in the following lines:

     ```
     Listen 23015
     Listen [::]:23015
     ```

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

   - `hsso.hostport` in *Common-Component-installation-folder*\conf\hsso.conf

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

   - `command.http.port` in `command_user.properties`

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

     For non-cluster systems:

     JP1/AO-installation-folder\conf

     For cluster systems:

     shared-folder-name\jp1ao\conf

   If the communication protocol is HTTPS:

   `Listen` and `VirtualHost` *`host-name`*`:`*`port-number`* in *Common-Component-installation-folder*\httpsd\conf\httpsd.conf

   Specify the new number in the place of 23016 in the following lines:

```
Listen 23016
Listen [::]:23016
<VirtualHost *:23016>
```

3. Execute the `hcmdsfwcancel` command to register exceptions to the firewall.

   In a cluster system, execute this command on both the active server and the standby server.

4. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` command with the `/start` option specified.

   For cluster systems:

   Use the cluster software to bring the service online.

5. Execute the `hcmdschgurl` command to update the URL.

Related topics

- *JP/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*
- 4.7 Procedure to change the URL

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

You can change the port number between JP1/AO and the SMTP server in the **Set Service Share Property** view.

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

1. Select **Service Share Properties** in the left pane of the **Administration** tab.

2. Select **SMTP server port number** from the right pane and click the **Set Service Share Property** button.

3. Enter the new port number and click the **OK** button.

Related topics

- *List of shared built-in service properties* in the *Job Management Partner 1/Automatic Operation Administration Guide*

4.6.3 Procedure to change the port number used to communicate with the task-processing engine

To change the port number used to communicate with the task-processing engine, you must edit the definition file for the task-processing engine and create the `ajscd_DNA.properties` file.

The default port number is 22250.

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 the execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), stop execution of the tasks or wait until the task status changes to the ended status.

To change the port number used to communicate with the task-processing engine:

1. Stop the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` command with the `/stop` option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.

2. Use a text editor to open the following task-processing engine definition file:
   %WinDir%\system32\drivers\etc\services

3. Update the value of the port number defined in `jp1ajs3cdinetd` in the open file, and save your changes.

4. Create a file named `ajscd_DNA.properties` in the following folder:
   JP1/AO-installation-folder\system\AJS3CD\conf

5. Add the following statement to the file you created, and then save the file.
   ajscd.port_number=*port-number-from-step-3*

6. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` 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 *Job Management Partner 1/Automatic Operation Administration Guide*

4.7 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 need to change the URL by using the `hcmdschgurl` command.

To change the URL:

The following examples show the steps for changing the URL from http://192.168.11.33:23015 to http://192.168.11.55:23015.

1. Execute the `hcmdschgurl` command with the `list` option specified to find the current URL.

   Example

   ```
   hcmdschgurl /list
   http://192.168.11.33:23015
   JP1/Automatic Operation
   ```

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

   Example

   ```
   hcmdschgurl /change "http://192.168.11.33:23015" "http://
   192.168.11.55:23015"
   The URL was changed from "http://192.168.11.33:23015" to "http://
   192.168.11.55:23015".
   ```

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

   Example

   ```
   hcmdschgurl /list
   http://192.168.11.55:23015
   JP1/Automatic Operation
   ```

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

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

To move the time forward on the JP1/AO server, you must stop and start 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 *Job Management Partner 1/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, or Terminated), 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 `hcmdssrv` command with the `/stop` option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.

3. Stop the JP1/Base service.

4. Move the time forward on the JP1/AO server.

5. Start the JP1/AO service.

   For non-cluster systems:

   Execute the `hcmdssrv` 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 *Job Management Partner 1/Automatic Operation Administration Guide*

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

To move the time back on the JP1/AO server, you must stop and start 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 *Job Management Partner 1/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 the execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), 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 `hcmdssrv` command with the `/stop` option specified.

   For cluster systems:

   Use the cluster software to bring the service offline.

3. Stop the JP1/Base service.

4. Note the current time indicated on the JP1/AO server.

5. Move the time back on the JP1/AO server.

6. Wait until the time you noted in step 4 is reached, and then start the service.

   For non-cluster systems:

   Execute the `hcmdssrv` 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 *Job Management Partner 1/Automatic Operation Administration Guide*

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 Set.	Optional	1.5 Installing JP1/AO Content Set

#

The procedure for installing JP1/AO depends on the current environment and the installation status of the product.

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	6.3 Procedure to perform an overwrite installation of JP1/AO (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 migrating an installation of JP1/AO that is operating in a non-cluster system environment to a cluster configuration is not supported.

Before installing JP1/AO, you need to install JP1/Base, which is prerequisite software. For details about how to install and set up JP1/Base, see the procedure in 5.3 Installing JP1/AO in a cluster system or 5.4 Installing JP1/AO in a cluster system (if Common Component is already installed in a cluster configuration).

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:
  - JP1/AJS3 - Manager
  - JP1/AJS3 - Agent
  - JP1/AJS2 - Manager
  - JP1/AJS2 - Agent
- OS and cluster software
  - The OS must be one of the following:
    - Windows Server 2008 R2 Enterprise
    - Windows Server 2008 R2 Datacenter
    - Windows Server 2012 Datacenter
    - Windows Server 2012 Standard
    - Windows Server 2012 R2 Datacenter
    - Windows Server 2012 R2 Standard
  - The cluster software must be Windows Server Failover Cluster (WSFC).
  - Patches and service packs required by JP1/AO and the cluster software must have been applied.
- 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 have been entered without the domain name. Because JP1/Base does not support FQDN-format host names, FQDN-format host names cannot be used in JP1/AO either.
- Environment variables
  The JP1/Base environment variable `JP1_HOSTNAME` must not be set as a system environment variable or a user environment variable. This might prevent the service from starting.

- 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.

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/Base and JP1/AO on the active server and standby server.	Required	5.3.3 Procedures for installing JP1/Base and 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	Register services by using the cluster software.	Required	5.3.6 Procedure to register services by using the cluster software

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 domain user with Administrator permissions on the OS and 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.
   - 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.

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

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

To install JP1/Base and 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/Base on the active server.

   For the JP1/Base installation destination, specify the same drive and folder names for the active server and standby server.

   After installation, if a message is displayed indicating that a restart is required, restart the active server.

3. Create a JP1 user in JP1/Base on the active server.

   For details, see 1.2.3 Creating a JP1 user in JP1/Base.

4. Install JP1/AO on the active server.

   - 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.
   - For the JP1/AO installation destination, specify the same drive and folder names for the active server and standby server.

   If a message is displayed indicating that a restart is required, restart the active server.

5. Install JP1/Base on the standby server.

   For the JP1/Base installation destination, specify the same drive and folder names for the active server and standby server.

   After installation, if a message is displayed indicating that a restart is required, restart the active server.

6. Create a JP1 user in JP1/Base on the standby server.

   For details, see 1.2.3 Creating a JP1 user in JP1/Base.

7. Install JP1/AO on the standby server.

   - 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.
   - For the JP1/AO installation destination, specify the same drive and folder names for the active server and standby server.

If a message is displayed indicating that a restart is required, restart the standby server.

Related topics

- 5.2 Installation prerequisites (for cluster systems)
- 1.2.3 Creating a JP1 user in JP1/Base
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*

5.3.4 Procedure for setting up the active server

Set up the active server.

To set up the active server:

1. If the **Current owner** of the resource group has been moved to the standby server, use the cluster software to move it to the active server.

2. Bring the resource group online by using the cluster software.

3. Set up the JP1/Base cluster environment on the active server.

   When you set up JP1/Base, specify the same logical host name as for JP1/AO.

   For the primary authentication server of the logical host name in JP1/Base, specify the same logical host name as for JP1/AO. If you specify a different authentication server, make sure that you can establish communication with that authentication server. In addition, make sure that the JP1 users registered on the authentication server satisfy the following constraints.

   - They must be able to be mapped to OS users.
   - They must have the permissions described in Table 1–2: JP1 user permission levels and have access to JP1 resource groups.

4. Create the cluster settings file (*Common-Component-installation-folder*\conf\cluster.conf) on the active server.

   For details, see 5.5 Cluster settings file (cluster.conf).

5. If the HAutomation Engine Web Service is running on the active server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.

6. Execute the `setupcluster` command on the active server.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base
- 5.5 Cluster settings file (cluster.conf)
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*
- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*

5.3.5 Procedure for setting up the standby server

Set up the standby server.

To set up the standby server:

1. Move **Current Owner** to the standby server by using the cluster software.
2. Set up the JP1/Base cluster environment on the standby server.

   When you set up JP1/Base, specify the same logical host name as for JP1/AO.

   For the primary authentication server of the logical host name in JP1/Base, specify the same logical host name as for JP1/AO. If you specify a different authentication server, make sure that you can establish communication with the authentication server you specify. In addition, make sure that the JP1 users registered on the authentication server satisfy the following constraints.

   - They must be able to be mapped to OS users.
   - They must have the permissions described in Table 1–2: JP1 user permission levels and have access to JP1 resource groups.
3. Create the cluster settings file (*Common-Component-installation-folder*\conf\cluster.conf) on the standby server.
4. If the HAutomation Engine Web Service is running on the standby server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.
5. Execute the `setupcluster` command on the standby server.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base
- 5.5 Cluster settings file (cluster.conf)
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*
- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*

5.3.6 Procedure to register services by using the cluster software

Register services by using the cluster software.

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 JP1/Base Event *logical-host-name*, set the dependency to the shared disk and client access point.

   Register 1 to 7 as service resources. Register 8 as a script resource.

   1. JP1/Base Event *logical-host-name*
   2. JP1/Base_*logical-host-name*
   3. HiRDB/ClusterService _HD0
   4. HBase Storage Mgmt Common Service
   5. HBase Storage Mgmt Web Service
   6. HAutomation Engine Web Service
   7. HAutomation Engine *logical-host-name*

8. `stopcluster` command

Here, *logical-host-name* means the logical host name specified in the cluster settings file.

If values are specified in **Startup Parameters** in the **General** Tab, remove the values.

For the `stopcluster` command, specify any value for the resource name and executable script name. Specify the `stopcluster` command to be executed only when this resource is placed offline. For details about how to specify the command, refer to the documentation of your cluster software.

Note that, if this resource is accidentally executed online, a KNAE01635-E message is output and task operation fails. In this case, stop JP1/AO, specify this resource to be executed only offline, and then restart JP1/AO.

3. Bring the resource group online by using the cluster software.

Related topics

- 5.6 Folders created on the JP1/AO shared disk
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*

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/Base and JP1/AO on the active and standby servers (if Common Component is already installed).	Required	5.4.3 Procedures for installing JP1/Base and 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 _HD0 offline.

5. On the active server, execute the `hcmdssrv` command with the `/stop` option specified to stop the JP1/AO service.

6. Use the cluster software to bring the HiRDB/ClusterService _HD0 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 _HD0 offline.

10. On the standby server, execute the `hcmdssrv` command with the `/stop` option specified to stop the JP1/AO service.

11. Use the cluster software to bring the HiRDB/ClusterService _HD0 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 *Job Management Partner 1/Automatic Operation Administration Guide*

5.4.3 Procedures for installing JP1/Base and JP1/AO on the active server and standby server (if Common Component is already installed)

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

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

1. Install JP1/Base on the active server.

   For the JP1/Base 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.

2. Create a JP1 user in JP1/Base on the active server.

   For details, see 1.2.3 Creating a JP1 user in JP1/Base.

3. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the active server.

4. 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 and JP1/AJS3 - Manager 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. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the standby server.

6. Install JP1/Base on the standby server.

   For the JP1/Base 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.

7. Create a JP1 user in JP1/Base on the standby server.

   For details, see 1.2.3 Creating a JP1 user in JP1/Base.

8. Use the cluster software to move the resource group where the Hitachi Command Suite products are registered to the standby server.

9. 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 and JP1/AJS3 - Manager 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.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*

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. Set up the JP1/Base cluster environment on the active server.

   When you set up JP1/Base, specify the same logical host name as for JP1/AO.

   For the primary authentication server of the logical host name in JP1/Base, specify the same logical host name as for JP1/AO. If you specify a different authentication server, make sure that you can establish communication with the authentication server you specify. In addition, make sure that the JP1 users registered on the authentication server satisfy the following constraints.

   - They must be able to be mapped to OS users.
   - They must have the permissions described in Table 1–2: JP1 user permission levels and have access to JP1 resource groups

3. If the HAutomation Engine Web Service is running on the active server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.

4. Execute the `setupcluster` command on the active server.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*
- *JP1/AO services* in the *Job Management Partner 1/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. Set up the JP1/Base cluster environment on the standby server.

   When you set up JP1/Base, specify the same logical host name as for JP1/AO.

   For the primary authentication server of the logical host name in JP1/Base, specify the same logical host name as for JP1/AO. If you specify a different authentication server, make sure that you can establish communication with the authentication server you specify. In addition, make sure that the JP1 users registered on the authentication server satisfy the following constraints.

   - They must be able to be mapped to OS users.
   - They must have the permissions described in Table 1–2: JP1 user permission levels and have access to JP1 resource groups

3. If the HAutomation Engine Web Service is running on the standby server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.

4. Execute the `setupcluster` command on the standby server.

Related topics

- 1.2.3 Creating a JP1 user in JP1/Base

- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*
- *JP1/AO services* in the *Job Management Partner 1/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 JP1/Base Event *logical-host-name*, set the dependency to the shared disk and client access point.

   Register 1 to 7 as service resources. Register 8 as a script resource.

   1. JP1/Base Event *logical-host-name*
   2. JP1/Base_*logical-host-name*
   3. HiRDB/ClusterService _HD0
   4. HBase Storage Mgmt Common Service
   5. HBase Storage Mgmt Web Service
   6. HAutomation Engine Web Service
   7. HAutomation Engine *logical-host-name*
   8. `stopcluster` command

   Here, *logical-host-name* means the logical host name specified in the cluster settings file.

   If values are specified in **Startup Parameters** in the **General** Tab, remove the values.

   For the `stopcluster` command, specify any value for the resource name and executable script name. Specify the `stopcluster` command to be executed only when this resource is placed offline. For details about how to specify the command, refer to the documentation of your cluster software.

   Note that, if this resource is accidentally executed online, a KNAE01635-E message is output and task operation fails. In this case, stop JP1/AO, specify this resource to be executed only offline, and then restart JP1/AO.

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)
- *Setting Up JP1/Base for Use in a Cluster System* in the *Job Management Partner 1/Base User's Guide*

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

Description

One specification key and setting can be specified per line.

> **Tip**
>
> For virtualhost, specify the same logical host name as the JP1/Base logical host name. Logical host names are case sensitive. If you specify logical host names that use a different combination of uppercase and lowercase letters, the `setupcluster` command will fail.

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

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 preset property definition files	*shared-folder-name*\jp1ao\extra_presets
	Folder for development service templates (plug-ins) and service template packages	*shared-folder-name*\jp1ao\develop
Common Component	Database installation folder	*shared-folder-name*\Base\database[#]
	Folder for setting up the active server	*shared-folder-name*\Base\online[#]
	Folder for setting up the standby server	*shared-folder-name*\Base\standby[#]
Task-processing engine	Folder for environment settings files	*shared-folder-name*¥jp1ao\JP1AJS2¥conf
	Folder for execution environment files	*shared-folder-name*¥jp1ao\JP1AJS2\database
	Folder for information files	*shared-folder-name*¥jp1ao\JP1AJS2\jobinf
	Log file output folder	*shared-folder-name*¥jp1ao\JP1AJS2\log
	Folder for system files	*shared-folder-name*¥jp1ao\JP1AJS2\sys
	Folder for working files	*shared-folder-name*¥jp1ao\JP1AJS2\tmp
	Folder for backup files	*shared-folder-name*¥jp1ao\JP1AJS2\backup

[#] If Common Component already exits in the cluster environment, a new folder is not created on the shared disk.

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)

6 Overwrite installation

This chapter explains how to perform an overwrite installation of JP1/AO.

6.1 Overwrite installation procedure

The term *overwrite installation* refers to installing the same version of a product in an environment where the product is already installed.

The overwrite installation procedure consists of the following steps.

Table 6–1: Overwrite installation procedure

Task		Required/ optional	Reference
1	Perform an overwrite installation of JP1/ Base.	Optional	*Installation and Setup* in the *Job Management Partner 1/Base User's Guide*
2	Perform an overwrite installation of JP1/ AO.	Required	For non-cluster systems: 6.2 Procedure to perform an overwrite installation of JP1/AO (non-cluster system) For cluster systems: 6.3 Procedure to perform an overwrite installation of JP1/AO (cluster system)
3	Perform an overwrite installation of JP1/ AO Content Set.	Optional	6.4 Overwrite installation of JP1/AO Content Set

6.2 Procedure to perform an overwrite installation of JP1/AO (non-cluster system)

You can use Hitachi Integrated Installer to perform overwrite installation of JP1/AO, as prompted by the wizard.

Note that the following files and folders are not overwritten during the overwrite installation:

JP1/AO-installation-folder\conf folder

- config_user.properties
- command_user.properties
- mailDefinition_ja.conf
- mailDefinition_en.conf
- mailDefinition_zh.conf

JP1/AO-installation-folder\conf\plugin folder

- charsetMapping_user.properties
- Files in the destinations folder

JP1/AO-installation-folder\docroot\help\ja folder

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\en folder

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\zh folder

- INDEX.HTM

Common-Component-installation-folder\CC\web\containers\AutomationWebService\webapps\Automation\services\custom folder

- All files in the above folder

To perform an overwrite installation:

1. Insert the distribution medium into the drive.
2. Continue the configuration process as prompted by the wizard.
   Specify the backup execution flag and the backup folder.
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, execute the `hcmdssrv` command with the `/start` option specified to start the JP1/AO service.

Related topics

- 1.2 Pre-installation tasks

6.3 Procedure to perform an overwrite installation of JP1/AO (cluster system)

In a cluster system, you must perform the overwrite installation of JP1/AO on both the active and standby servers.

The overwrite installation procedure consists of the following steps.

Table 6–2: Overwrite installation procedure (cluster system)

Task		Required/ optional	Reference
1	Perform the tasks that must be completed in advance.	Required	6.3.1 Tasks that must be completed before an overwrite installation (cluster system)
2	Configure services before starting the overwrite installation.	Required	6.3.2 Procedure to configure services before an overwrite installation (cluster system)
3	Perform an overwrite installation of JP1/AO on the active server.	Required	6.3.3 Procedure to perform an overwrite installation of JP1/AO on the active server (cluster system)
4	Perform an overwrite installation of JP1/AO on the standby server.	Required	6.3.4 Procedure to perform an overwrite installation of JP1/AO on the standby server (cluster system)
5	Enable failover of the resource group.	Required	6.3.5 Procedure for enabling failover of the resource group (cluster system)

Related topics

- 5.2 Installation prerequisites (for cluster systems)

6.3.1 Tasks that must be completed before an overwrite installation (cluster system)

Before you perform an overwrite installation of JP1/AO, you must perform the tasks listed below.

Before you begin

Log in to the JP1/AO server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

Note that the following files are not overwritten during the overwrite installation:

shared-folder-name\conf folder

- config_user.properties
- command_user.properties
- mailDefinition_ja.conf
- mailDefinition_en.conf
- mailDefinition_zh.conf

shared-folder-name\conf\plugin folder

- charsetMapping_user.properties

JP1/AO-installation-folder\docroot\help\ja folder

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\en folder

- INDEX.HTM

JP1/AO-installation-folder\docroot\help\zh folder

- INDEX.HTM

Common-Component-installation-folder\CC\web\containers\AutomationWebService\webapps\Automation\services\custom folder

- All files in the above folder

6.3.2 Procedure to configure services before an overwrite installation (cluster system)

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 Response, Abnormal Detection, or Terminated), 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
   - JP1/Base_*logical-host-name*
   - JP1/Base Event _*logical-host-name*

   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*
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - `stopcluster` command#

5. On the active server, execute the `hcmdssrv` 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
   - JP1/Base_*logical-host-name*
   - JP1/Base Event _*logical-host-name*

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
   - JP1/Base_*logical-host-name*
   - JP1/Base Event _*logical-host-name*

   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*
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - `stopcluster` command#
10. On the standby server, execute the `hcmdssrv` 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
    - JP1/Base_*logical-host-name*
    - JP1/Base Event _*logical-host-name*
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 if an overwrite installation is performed in a cluster environment created in JP1/AO 10-10 or an earlier version.

Related topics

- *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*

6.3.3 Procedure to perform an overwrite installation of JP1/AO on the active server (cluster system)

Perform an overwrite installation of JP1/AO on the active server.

To perform an overwrite 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 service (JP1/Base_*logical-host-name*) is online on the active server, bring it offline.

3. Start the service (JP1/Base) on the active server.

4. Perform an overwrite installation of JP1/AO on the active server.

5. In the **Tasks** window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), stop execution of the tasks, or wait until task status changes to the ended status.

6. If the HAutomation Engine Web Service is running on the active server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.

7. Execute the `setupcluster` command on the active server.

6.3.4 Procedure to perform an overwrite installation of JP1/AO on the standby server (cluster system)

Perform an overwrite installation of JP1/AO on the standby server.

To perform an overwrite 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. If the service (JP1/Base_*logical-host-name*) is online on the standby server, bring it offline.

3. Start the service (JP1/Base) on the standby server.

4. Perform an overwrite installation of JP1/AO on the standby server.

5. In the Tasks window, check the tasks. If any tasks are in execution status (In Progress, Waiting for Response, Abnormal Detection, or Terminated), stop execution of the tasks or wait until the task status changes to the ended status.

6. If the HAutomation Engine Web Service is running on the standby server, stop it by executing the `hcmdssrv` command with the `/stop /server AutomationWebService` option specified.

7. Execute the `setupcluster` command on the standby server.

6.3.5 Procedure for enabling failover of the resource group (cluster system)

Enable failover of the resource group.

Important note

- If you want to perform an upgrade installation in a cluster environment created in JP1/AO 10-00, you must change the display name of the resource registered in the cluster software from JP1/AJS2_*logical-host-name* to HAutomation Engine *logical-host-name* before enabling failover.

- If you want to perform an overwrite installation in a cluster environment created in JP1/AO 10-10 or an earlier version, add a script resource that allows a user to execute the `stopcluster` command. Specify the dependency of the added script resource after HAutomation Engine *logical-host-name*.

  For the `stopcluster` command, specify any value for the resource name and executable script name. Specify the `stopcluster` command to be executed only when this resource is placed offline. For details about how to specify the command, refer to the documentation of your cluster software.

  If this resource is accidentally executed online, a KNAE01635-E message is output and task operation fails. In this case, stop JP1/AO, specify this resource to be executed only offline, and then restart JP1/AO.

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.

6.4 Overwrite installation of JP1/AO Content Set

6.4.1 Procedure to perform an overwrite installation of JP1/AO Content Set

The following describes how to perform an overwrite installation of JP1/AO Content Set. When an overwrite installation of JP1/AO Content Set is performed, the previous version of Service Template Set is overwritten by the latest one.

Before you begin

- Log in to the server as a user with Administrator permissions.
- Confirm that JP1/AO is installed.

  Note that because JP1/AO Content Set 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 Set installation folder are deleted during overwrite installation. Back up the necessary files and folders.

To perform an overwrite installation of JP1/AO Content Set:

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

   Do not install JP1/AO Content Set 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.

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 Set

  Version:

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

  JP1/AO-Content-Set-installation-folder\contents\setup

  You can use the**Add Service** dialog box or the `listservices` command to confirm that the service templates have been imported.

7 Upgrade Installation

This chapter explains how to perform an upgrade installation of JP1/AO.

7.1 Upgrade installation procedure

The term *upgrade installation* refers to installing a later version of a product in an environment where the product is already installed.

Important note

When you perform an upgrade installation in an environment of JP1/AO 10-00, you must uninstall JP1/AJS3 - View from that environment. However, do not uninstall service templates created in an environment of 10-00. Such service templates might be used for migration to a service template editor.

Do not uninstall JP1/AJS3 - Manager. If you uninstall JP1/AJS3 - Manager, the upgrade installation will fail.

An upgrade installation follows the procedure shown below.

Table 7–1: Upgrade installation procedure

Task		Required/optional	Reference
1	Perform an overwrite installation with a later version of JP1/AO.	Required	For non-cluster systems: 6.2 Procedure to perform an overwrite installation of JP1/AO (non-cluster system) For cluster systems: 6.3 Procedure to perform an overwrite installation of JP1/AO (cluster system)
2	Perform an overwrite installation with a later version of JP1/AO Content Set.	Optional	6.4 Overwrite installation of JP1/AO Content Set

8 Uninstallation

This chapter explains how to uninstall JP1/AO.

8.1 Uninstallation procedure

After uninstalling JP1/AO, you must manually uninstall JP1/AO - Contents and JP1/AO Content Set.

Important note

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 8–1: Uninstallation procedure

Task		Required/ optional	Reference
1	Prepare for uninstallation.	Required	8.2 Prepare for uninstallation
2	Uninstall JP1/AO and related products.	Required	For non-cluster systems: 8.3 Procedure to uninstall JP1/AO (non-cluster system) For cluster systems: 8.4 Procedure to uninstall JP1/AO (cluster system)
3	Uninstall JP1/Base.#	Optional	*Uninstalling JP1/Base* in the *Job Management Partner 1/Base User's Guide*

#

You cannot uninstall JP1/Base independently. To uninstall JP1/Base, you must first uninstall JP1/AO.

Do not install other products during the uninstallation of JP1/AO.

8.2 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 both Administrator permissions and the JP1/AO Admin role, 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 the relevant service is **Disabled**, uninstallation will fail because the service cannot be started. Set **Startup type** to **Automatic** or **Manual**.

  For details about the JP1/AO service, see *JP1/AO services* in the *Job Management Partner 1/Automatic Operation Administration Guide*.
- When you uninstall JP1/AO, the JP1/Base services are started. If you are controlling the order in which services start in JP1/Base, make sure that there is no problem when the services start.

Related topics

- 8.1 Uninstallation procedure
- 8.3 Procedure to uninstall JP1/AO (non-cluster system)
- 8.4 Procedure to uninstall JP1/AO (cluster system)

8.3 Procedure to uninstall JP1/AO (non-cluster system)

Uninstallation of JP1/AO is initiated from **Programs and Features** in the **Control Panel**.

To uninstall JP1/AO:

1. In the Windows **Control Panel**, click **Programs** and then **Programs and Features**. In the window that appears, select JP1/AO, and then click **Uninstall**.
2. Specify whether to start services after uninstallation is complete, as prompted by the wizard.
3. Uninstall JP1/AO.
4. Uninstall JP1/AO - Contents and JP1/AO Content Set.

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 note**
>
> 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 `hcmdsintg` command.

Results of procedure

- **JP1_Automatic Operation** is removed from **All Programs** in the **Start** menu.
- If Common Component is also uninstalled when JP1/AO is uninstalled, programs for which firewall exceptions were registered are released.

Related topics

- 8.1 Uninstallation procedure
- 8.2 Prepare for uninstallation
- 8.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Set

8.4 Procedure to uninstall JP1/AO (cluster system)

In a cluster system, you must uninstall JP1/AO from both the active server and standby server.

After JP1/AO is uninstalled, JP1/Base can be used in a physical host configuration.

The procedure to uninstall JP1/AO consists of the following steps.

Table 8–2: Uninstallation procedure

Task		Required/ optional	Reference
1	Prepare for uninstallation.	Required	8.4.1 Procedure to configure services before uninstallation (cluster system)
2	Uninstall JP1/AO and related products.	Required	8.4.2 Procedure to uninstall JP1/AO and related products (cluster system)
3	Delete folders created in the shared folder.	Required	8.4.3 Procedure to delete folders created in the shared folder (cluster system)
4	Delete services from the cluster software.	Required	8.4.4 Procedure to delete services from the cluster software (cluster system)
5	Configure JP1/Base.	Required	8.4.5 Procedure to configure JP1/Base (cluster system)

Related topics

- 8.1 Uninstallation procedure
- 8.2 Prepare for uninstallation

8.4.1 Procedure to configure services before uninstallation (cluster system)

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 Response, Abnormal Detection, or Terminated), 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
   - JP1/Base_*logical-host-name*

- JP1/Base Event *_logical-host-name*

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*
- HBase Storage Mgmt Common Service
- HBase Storage Mgmt Web Service
- `stopcluster` command

5. On the active server, execute the `hcmdssrv` 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
   - JP1/Base*_logical-host-name*
   - JP1/Base Event *_logical-host-name*

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 _HD0
   - JP1/Base*_logical-host-name*
   - JP1/Base Event *_logical-host-name*

   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*
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - `stopcluster` command

10. On the standby server, execute the `hcmdssrv` 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
    - JP1/Base*_logical-host-name*
    - JP1/Base Event *_logical-host-name*

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.

8.4.2 Procedure to uninstall JP1/AO and related products (cluster system)

Uninstall JP1/AO and related products. You must uninstall JP1/AO, JP1/AO - Contents, and JP1/AO Content Set.

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. On the active server, uninstall the database by executing the `ajsembdbuninstl -mh` *logical-host-name* command.#1
3. Uninstall JP1/AO from the active server.

   After uninstallation, manually delete any files remaining in the JP1/AO installation folder. If JP1/AO has been upgraded from version 10-00, also check for files remaining in the folder containing the task-processing engine system files#2, and then manually delete any remaining files.
4. Delete the JP1/Base logical host from the active server.
5. Uninstall JP1/AO - Contents and JP1/AO Content Set from the active server.

   After uninstallation, manually delete any files remaining in the JP1/AO - Contents and JP/AO Content Set installation folder.
6. Use the cluster software to move the resource group where the JP1/AO service is registered to the standby server.
7. On the standby server, uninstall the database by executing the `ajsembdbuninstl -mh` *logical-host-name* command.#1
8. Uninstall JP1/AO from the standby server.

   After uninstallation, manually delete any files remaining in the JP1/AO installation folder. If you have performed an upgrade installation of JP1/AO from version 10-00, also check for files remaining in the folder containing the task-processing engine system files#2, and then manually delete any remaining files.
9. Delete the JP1/Base logical host from the standby server.
10. Uninstall JP1/AO - Contents and JP1/AO Content Set from the standby server.

    After uninstallation, manually delete any files remaining in the JP1/AO - Contents and JP/AO Content Set installation folder.

#1

Commands whose name begins with `ajs` are contained in the folder for task-processing engine system files. For details, see A.1 List of folders.

#2

For details about the folder for task-processing engine system files, see A.1 List of folders.

Related topics

- 8.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Set
- *Deleting logical hosts* in the *Job Management Partner 1/Base User's Guide*

8.4.3 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:

1. Delete the following folders created in the shared folder:
   - *shared-folder-name*\jp1ao
   - *shared-folder-name*\Base#

   #

   Do not delete this folder if other Hitachi Command Suite products are installed.

8.4.4 Procedure to delete services from the cluster software (cluster system)

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:
   - JP1/Base Event *logical-host-name*
   - JP1/Base_*logical-host-name*
   - HAutomation Engine Web Service
   - HAutomation Engine *logical-host-name*
   - HBase Storage Mgmt Common Service
   - HBase Storage Mgmt Web Service
   - HiRDB/ClusterService _HD0
   - `stopcluster` command
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.

8.4.5 Procedure to configure JP1/Base (cluster system)

Configure JP1/Base.

To configure JP1/Base:

1. On both the active and standby servers, if you want to use JP1/Base as the physical host, change the communication binding method to the ANY binding method.

Important note

If Common Component and JP1/AO are on different servers, a warning message is output when 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 `hcmdsintg` command.

Related topics

- *Changing communication settings* in the *Job Management Partner 1/Base User's Guide*

8.5 Procedure to uninstall JP1/AO - Contents and JP1/AO Content Set

When JP1/AO is uninstalled, JP1/AO - Contents and JP1/AO Content Set are not automatically removed. Therefore, you must uninstall them manually. You can uninstall JP1/AO - Contents and JP1/AO Content Set from **Programs and Features** in the Control Panel.

Before you begin

The JP1/AO - Contents and JP1/AO Content Set installation folders and the user-created files and folders contained in them are all deleted during uninstallation. Back up necessary files and folders.

To uninstall JP1/AO - Contents and JP1/AO Content Set:

1. In the Windows **Control Panel**, click **Programs** and then **Programs and Features**. In the window that appears, select **JP1/Automatic Operation - Contents** or **JP1/Automatic Operation Content Set**, and then click **Uninstall**.

2. Uninstall JP1/AO - Contents or JP1/AO Content Set, as prompted by the wizard.

Related topics

- 1.5.2 JP1/AO Content Set installation folder

9 Server Migration

This chapter explains how to migrate the environment in JP1/AO.

9.1 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, and revisions)
- No tasks must be in the In Progress, Waiting for Response, Abnormal Detection, or Terminated status on the original JP1/AO server.
- JP1/Base and JP1/AO must not be installed on the target server.

When to restore JP1/Base, which is a prerequisite product of JP1/AO, depends on whether the original JP1/AO server has been upgraded from version 10-00.

- If the JP1/AO server has been upgraded from version 10-00.:
  Restore JP1/Base before you start the JP1/AO restore operation.
- If the JP1/AO server has not been upgraded from version 10-00.:
  Restore JP1/Base as part of the JP1/AO restore operation.

The following describes the migration procedure depending on whether the original JP1/AO server has been upgraded.

If the JP1/AO server has not been upgraded from version 10-00:

Table 9–1: Migration procedure (if the original JP1/AO server has not been upgraded from version 10-00)

Task		Reference
1	Back up JP1/AO on the original server.	Topics about backup in the *Job Management Partner 1/Automatic Operation Administration Guide*
2	Install JP1/Base and JP1/AO on the target server. Make sure that the following items match on the original server and the target server: • JP1/Base installation folder • JP1/AO installation folder • OS user accounts that have been mapped to JP1 users	For non-cluster systems: 1.1 New installation procedure For cluster systems: 1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base, 1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2), 5.1 Procedure for installing JP1/AO in a cluster system
3	Restore JP1/AO on the target server.	Topics about restoration in the *Job Management Partner 1/Automatic Operation Administration Guide*
4	Make sure that the target server is running, and then start operations.	--

Legend:

--: None

If the JP1/AO server has been upgraded from version 10-00:

Table 9–2: Migration procedure (if the original JP1/AO server has been upgraded from version 10-00)

Task		Reference
1	Back up JP1/AO on the original server.	Topics about backup in the *Job Management Partner 1/Automatic Operation Administration Guide*
2	Install and restore JP1/Base on the target server. Make sure that the following items match on the original server and the target server: • JP1/Base installation folder • OS user accounts that have been mapped to JP1 users	1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base
3	Install JP1/AO on the target server. At this time, JP1/AO must be installed in the same folder as the installation folder on the original server.	For non-cluster systems: 1.1 New installation procedure For cluster systems: 1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base, 1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2), 5.1 Procedure for installing JP1/AO in a cluster system
4	Restore JP1/AO on the target server. There is no need to restore JP1/Base because it has been restored in step 2.	Topics about restoration in the *Job Management Partner 1/Automatic Operation Administration Guide*
5	Make sure that the target server is running, and then start operations.	--

Legend:

--: None

9.2 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:
  - System locale
  - The environment for Hitachi Command Suite products (configuration, version, and revision)
- No tasks must be in the In Progress, Waiting for Response, Abnormal Detection, or Terminated status on the original JP1/AO server.
- JP1/Base and JP1/AO must not be installed on the target server.

When to restore JP1/Base, which is a prerequisite product of JP1/AO, depends on whether the original JP1/AO server has been upgraded from version 10-00..

- If the JP1/AO server has been upgraded from version 10-00.:
  Restore JP1/Base before you start the JP1/AO restore operation.
- If the JP1/AO server has not been upgraded from version 10-00.:
  Restore JP1/Base as part of the JP1/AO restore operation.

The following describes the migration procedure depending on whether the original JP1/AO server has been upgraded.

If the JP1/AO server has not been upgraded from version 10-00:

Table 9–3: Migration procedure (if the original JP1/AO server has not been upgraded from version 10-00)

Task		Reference
1	Back up JP1/AO on the original server.	Topics about backup in the *Job Management Partner 1/Automatic Operation Administration Guide*
2	Change the host name and IP address of the target server to match the migration source environment.	--
3	Install JP1/Base and JP1/AO on the target server. Make sure that the following items match on the original server and the target server: • JP1/Base installation folder • JP1/AO installation folder • OS user accounts that have been mapped to JP1 users	For non-cluster systems: 1.1 New installation procedure For cluster systems: 1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base, 1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2), 5.1 Procedure for installing JP1/AO in a cluster system
4	Restore JP1/AO on the target server.	Topics about restoration in the *Job Management Partner 1/Automatic Operation Administration Guide*

Task		Reference
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.	- 4.4 Procedure to change the host name of the JP1/AO server - 4.5 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

If the JP1/AO server has been upgraded from version 10-00:

Table 9–4: Migration procedure (if the original JP1/AO server has been upgraded from version 10-00)

Task		Reference
1	Back up JP1/AO on the original server.	Topics about backup in the *Job Management Partner 1/Automatic Operation Administration Guide*
2	Change the host name and IP address of the target server to match the migration source environment.	--
3	Install and restore JP1/Base on the target server. Make sure that the following items match on the original server and the target server: - JP1/Base installation folder - OS user accounts that have been mapped to JP1 users	1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base
4	Install JP1/AO on the target server. At this time, JP1/AO must be installed in the same folder as the installation folder on the original server.	For non-cluster systems: 1.1 New installation procedure For cluster systems: 1.2.2 Installing JP1/Base, 1.2.3 Creating a JP1 user in JP1/Base, 1.2.4 Installing. NET Framework (Windows Server 2012 or Windows Server 2012 R2), 5.1 Procedure for installing JP1/AO in a cluster system
5	Restore JP1/AO on the target server. There is no need to restore JP1/Base because it has been restored in step 3.	Topics about restoration in the *Job Management Partner 1/Automatic Operation Administration Guide*
6	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.	- 4.4 Procedure to change the host name of the JP1/AO server - 4.5 Procedure to change the IP address of the JP1/AO server
7	Make sure that the target server is running, and then start operations.	--

Legend:

--: None

10 Troubleshooting During Setup

This chapter explains what to do if problems occur in JP1/AO.

10.1 What to do if an attempt to set execution agents for the task-processing engine fails

If the KNAE04326-E message appears and an attempt to set execution agents for the task-processing engine fails during installation, the JP1 user might not have the required permissions. In this case, perform the following procedure.

Procedure

1. Execute the following command to start the JP1/AO service.

   Common-Component-installation-folder`\bin\hcmdssrv /start`

2. Execute the following command to set the JP1 user with JP1_AO_Admin permission, JP1_AJS_Manager permission, and JP1_JPQ_Admin permission assigned in the JP1_USERNAME environment variable.

   `set JP1_USERNAME=`*JP1-user-name*

3. Make sure that the HAutomation Engine service is running, and execute the following command to confirm the execution agent settings.

   `ajsagtshow -l`#

   Check the results of the command to see if all the conditions listed below are satisfied. If any condition is not satisfied, go to step 4 and change the execution agent settings. If all conditions are satisfied, steps 4 to 7 are unnecessary. Go to step 8.

   - The value of CON-EXE for @SYSTEM is 50.
   - The AGENT items contain `loop`.
   - The AGENT items contain `userResponse`.

4. If the value of CON-EXE for @SYSTEM is not 50, execute the following command to change the maximum number of concurrently executable jobs for the execution agent.

   `ajsagtalt -a @SYSTEM -c 00:00-00:00=50`#

5. If the AGENT items do not contain `loop`, execute the following command to add `loop` to the execution agent settings.

   `ajsagtadd -a loop -s` *command-execution-host-name* `-c 00:00-00:00=20`#

6. If the AGENT items do not contain `userResponse`, execute the following command to add `userResponse` to the execution agent settings.

   `ajsagtadd -a userResponse -s` *command-execution-host-name* `-c 00:00-00:00=70`#

7. Execute the following command to back up the JP1/AO system with the new execution agent settings.

   `backupsystem /dir` *path-to-backup-data* `/auto`#

   Important note

   If you execute the `restoresystem` command to restore the system from the existing backup data without backing up the new execution agent settings, the JP1/AO system will return to the status that existed before the execution agent was changed.

8. Change the JP1 user to the user to which you assigned permissions in step 2.

   For details about how to change a JP1 user, see 4.2 Procedure to change a JP1 user.

#

For details about the location of the command, see A.1 List of folders. Commands whose name begins with `ajs` are stored in the folder for task-processing engine system files.

Related topics

- *Messages KNAE04000 through KNAE04999* in the manual *Job Management Partner 1/Automatic Operation Messages*

10.2 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 `hcmdsgetlogs` 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

The table below lists the folders that are created when JP1/AO is installed.

In the table, the default value for *JP1/AO-installation-folder* as shown below:

system-drive\Program Files (x86)\Hitachi\JP1AO

Table A–1: List of folders created during the installation

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\extra_presets	Folder for additional preset property definition 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\system\JP1AJS2	Folder for task-processing engine system files#1
JP1/AO-installation-folder\webapps	Working folder used by JP1/AO internal commands
JP1/AO-installation-folder\work	Working folder
system-drive\Program Files (x86)\Hitachi\HiCommand\Base#2	Common Component installation folder

#1

This folder also contains commands whose name begins with `ajs`, which are executed by the task-processing engine. These commands are stored in *JP1/AO-installation-folder*\system\JP1AJS2\bin or *JP1/AO-installation-folder*\system\JP1AJS2\tools. Note, however, that if JP1/AO has been upgraded from version 10-00, these commands are stored in the folder that was specified by the user before the upgrade.

#2

If JP1/AO is installed in an environment where the Hitachi Command Suite products are installed, this folder is not created. This is because Common Component has already been installed in the folder that was created when the Hitachi Command Suite products were installed.

A.2 Version changes

(1) Changes in version 10-10

- 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.
- Thecharacter-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.

Index