

Job Management Partner 1 Version 10

**Job Management Partner 1/Automatic Operation
Administration Guide**

3021-3-314-20(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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware and vCenter Server are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

VMware and VMware vSphere ESX are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

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

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

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

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

This product includes software developed by Andy Clark.

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

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

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

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

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

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

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

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

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

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



Job Management Partner 1/Automatic Operation includes RSA BSAFE(R) Cryptographic software of EMC Corporation.

HITACHI
Inspire the Next

 Hitachi, Ltd.





■ **Issued**

Dec. 2014: 3021-3-314-20(E)

■ **Copyright**

All Rights Reserved. Copyright (C) 2012, 2014, Hitachi, Ltd.

Summary of amendments

The following table lists changes in this manual (3021-3-314-20(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: <i>Job Management Partner 1/Automatic Operation GUI and Command Reference</i> (3021-3-315(E)) After the change: <i>Job Management Partner 1/Automatic Operation GUI, Command, and API Reference</i> (3021-3-366(E))	--
Windows Server 2012 R2 was added as an applicable OS.	--
As an external authentication linkage, the function for linking with Active Directory was added.	1.2,1.15,8.9,10.3,10.4
The function to forcibly stop tasks was added.	1.6,1.6.7,6.10.2
The function to retry steps was added.	1.6,1.6.8,6.11.2,6.11.3
Task progress can now be checked in the Task Monitor view.	1.6.13,6.3.1
A description about the maximum number of plug-ins contained in a task that can be executed concurrently was added.	1.6.14
Public key authentication was added as a method of authentication with devices to be used.	1.7.2,1.12.3,1.12.6,13.1,13.5
The maximum number of preset properties you can add to a service template can now be changed in the property file (config_user.properties).	1.8.1
Whether to elevate to a superuser can now be specified for the general command plug-in, file-forwarding plug-in, and content plug-in.	1.12.3
Detailed task information can now be output in a batch, and scheduled tasks and recurring tasks can now be registered in a batch.	1.13.1,6.15,6.16,12.1,12.3
The HTTPS protocol can now be used for connection between the JP1/AO server and Web browser.	1.19.1,2.1,12.3,12.4
Procedures for displaying and downloading task logs were added.	6.4,6.5,13.2
A description that the following files are no longer backed up or restored by using commands was added: <ul style="list-style-type: none"> • SSL server certificate files for HTTPS connection • Private key files for HTTPS connection • Private key files for public keys 	12.1,12.2,12.3,12.4
The <code>stopcluster</code> command was added. Preparation for stopping JP1/AO services in a cluster environment can now be performed.	12.2,12.4,12.6,12.10
A description about the procedure for restoring the JP1/AO server remotely by using backup files was added.	12.11
Actions to take when a task does not stop were changed.	13.4

Changes	Location
Task log output contents were changed. Also, a description about return values of plug-ins to be recorded in a task log file was added.	13.9.3

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

Preface

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

In this manual, Job Management Partner 1 is abbreviated as *JP1*, and Job Management Partner 1/Automatic Operation is abbreviated as *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 want to know how to use JP1/AO systems
- Users who wish to execute services in a JP1/AO system

■ 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	
	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

This section describes the conventions used in this manual.

Text formatting	Description
<i>Character string</i>	Italic characters indicate a variable. Example: A date is specified in <i>YYYYMMDD</i> 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

Notices 2

Summary of amendments 5

Preface 7

1 Using JP1/AO 15

1.1 Overview of JP1/AO operation 16

1.1.1 Basic tasks in a preparation phase 16

1.1.2 Basic tasks in day-to-day operation 18

1.1.3 Basic tasks in maintenance phase 18

1.1.4 Basic tasks in review phase and post-review preparation phase 19

1.2 List of JP1/AO features 20

1.3 Managing service templates 22

1.3.1 Service template versions 23

1.3.2 Storage location of service templates in JP1/AO standard-package plug-ins and JP1/AO Content Set 23

1.4 Managing services 25

1.4.1 Intervening actions while defining services 26

1.4.2 Intervening action when submitting a service 27

1.5 Submitting services for execution 29

1.5.1 Timing of executing services 30

1.5.2 Process of recurring execution 31

1.5.3 Using JP1/AO in time zones affected by daylight saving 32

1.6 Managing tasks 33

1.6.1 Overview of task management 35

1.6.2 Managing schedules 37

1.6.3 Managing task progress 38

1.6.4 Behavior when tasks are stopped 41

1.6.5 Behavior when tasks waiting for a response have stopped 42

1.6.6 Behavior when a task has stopped while repeated execution plug-ins are running 42

1.6.7 Behavior when a task is forcibly stopped 43

1.6.8 Retrying tasks 44

1.6.9 Archiving tasks and removing histories automatically 45

1.6.10 Display format of task summary 46

1.6.11 Task categories and generation timing 47

1.6.12 Task statuses and status transitions 48

1.6.13 Step statuses 50

1.6.14 Maximum number of plug-ins contained in a task that can be executed concurrently 51

1.6.15	Retention periods for task histories	52
1.7	Setting shared service properties	53
1.7.1	Notes on setting shared service properties	54
1.7.2	List of shared built-in service properties	54
1.8	Setting preset properties	57
1.8.1	About preset property definition files	57
1.8.2	Preset property definition file format	57
1.9	Assigning categories	59
1.10	Managing users	61
1.10.1	Default user in JP1/AO	62
1.10.2	Setting password criteria	62
1.11	Managing groups	64
1.11.1	Access control using user groups and resource groups	65
1.11.2	Relationship between resource groups and user groups	66
1.11.3	Built-in resource groups and built-in user groups	67
1.11.4	Types of roles that can be set for resource groups	68
1.11.5	Relationship between resource groups and shared service properties	68
1.12	Managing connection destination	70
1.12.1	Access control using connection destination management	70
1.12.2	Configuring JP1/AO to reference authentication information of connection destination definitions	73
1.12.3	List of definition parameters for connection destinations	73
1.12.4	Resolving host names to IP addresses	75
1.12.5	Entry format for connection destinations	77
1.12.6	Default connection destinations	78
1.13	Maintenance	79
1.13.1	Notes on backup and restoration	79
1.13.2	Notes on restarting JP1/AO services	80
1.13.3	Data that is restored	80
1.14	Linking with JP1/Base authentication	82
1.15	Linking with Active Directory	83
1.16	Linking with JP1/IM event monitoring	85
1.16.1	Timing of JP1 event reporting	86
1.17	Linking with JP1/AJS3	87
1.18	Email notification	88
1.18.1	List of email notification settings	88
1.19	Direct-access URLs	90
1.19.1	Format and parameters of direct-access URLs	90
1.19.2	How to estimate the number of characters in a query parameter	93
1.20	Configuring Link&Launch	94
1.21	Linking with JP1/IM - NP business content	95

2	Logging in to JP1/AO	96
2.1	Logging in to JP1/AO	97
3	Managing service templates	99
3.1	Developing service templates	100
3.2	Adding (importing) a service template to JP1/AO	101
3.3	Deleting service templates from JP1/AO	102
3.4	Adding preset properties to service templates	103
3.5	Outputting (exporting) service template lists	104
4	Managing services	105
4.1	Adding services	106
4.2	Editing services	108
4.3	Deleting services	109
4.4	Outputting (exporting) a list of services	110
5	Executing Services	111
5.1	Submitting services for immediate execution	112
5.2	Submitting services for execution at a specified time	113
5.3	Submitting services for recurring execution	114
6	Managing Tasks	116
6.1	Checking the status of tasks executed by the logged-in user	117
6.2	Checking the status of all tasks	118
6.3	Checking the progress of a task	119
6.3.1	Checking the progress of tasks in flow format	119
6.3.2	Checking the progress of tasks in a list	120
6.4	Displaying task logs	122
6.5	Downloading task log files	123
6.6	Entering actions for tasks waiting for a response (entering responses)	124
6.7	Suspending tasks (suspending schedules)	126
6.8	Resuming suspended tasks (resuming schedules)	127
6.9	Canceling tasks (canceling schedules)	128
6.10	Stopping tasks (execution stop)	129
6.10.1	Stopping tasks (execution stop)	129
6.10.2	Stopping tasks (forced stop)	130
6.11	Redoing tasks	131
6.11.1	Re-executing tasks	131
6.11.2	Retrying tasks from failed steps	132
6.11.3	Retrying tasks from the step after the failed one	133
6.12	Moving tasks to the History list (archiving tasks)	134
6.13	Deleting task histories	135

6.14	Outputting task lists (exporting tasks)	136
6.15	Outputting detailed task information in a batch	137
6.16	Re-registering scheduled tasks and recurring tasks in a batch	138
7	Setting service share properties	139
7.1	Procedure for setting service share properties	140
8	Managing Users	141
8.1	Registering users in JP1/AO	142
8.2	Setting of another user's information by an administrator	143
8.3	Setting one's own user information	144
8.4	Changing of another user's password by an administrator	145
8.5	Changing one's own password	146
8.6	Changing the User Management permission settings	147
8.7	Locking users	148
8.8	Unlocking users	149
8.9	Changing the user authentication method	150
8.10	Deleting users from JP1/AO	151
9	Managing Resource Groups	152
9.1	Creating resource groups	153
9.2	Editing resource groups	154
9.3	Deleting resource groups	155
10	Managing User Groups	156
10.1	Creating user groups	157
10.2	Editing user groups	158
10.3	Registering Active Directory groups linking with JP1/AO	159
10.4	Assigning resource groups and roles to user groups	160
10.5	Changing the user groups to which a user belongs	161
10.6	Deleting user groups	162
11	Managing Connection Destinations	163
11.1	Defining connection destinations	164
11.2	Editing the definition information for connection destinations	165
11.3	Deleting connection destinations	166
12	Maintenance	167
12.1	Backing up data in a JP1/AO system (non-cluster configuration)	168
12.2	Backing up data in a JP1/AO system (cluster configuration)	170
12.3	Restoring data in a JP1/AO system (non-cluster configuration)	173
12.4	Restoring data in a JP1/AO system (cluster configuration)	175
12.5	Database maintenance (non-cluster configuration)	179

12.6	Database maintenance (cluster configuration)	181
12.7	Starting a JP1/AO system (non-cluster configuration)	184
12.8	Starting a JP1/AO system (cluster configuration)	185
12.9	Stopping a JP1/AO system (non-cluster configuration)	186
12.10	Stopping a JP1/AO system (cluster configuration)	187
12.11	Restoring JP1/AO servers remotely by using backup files	188

13 Troubleshooting JP1/AO 192

13.1	Types of problem	193
13.2	When a running task fails	194
13.3	Taking time to complete tasks	195
13.4	When a task does not end	196
13.5	Public key authentication with connection destinations fails	197
13.6	When you cannot connect to the JP1/AO GUI	198
13.7	When you cannot log in to JP1/AO	199
13.8	When JP1/AO will not start	200
13.9	Detailed description of log information	201
13.9.1	Format of log entries	201
13.9.2	Collecting log information	202
13.9.3	Task log details	203
13.9.4	Integrated trace log and event log details	206
13.9.5	Public log details	206

Appendix 208

A	Reference Information	209
A.1	List of JP1 events output by JP1/AO	209
A.2	Outputting audit log entries	215
A.3	JP1/AO services	223
A.4	Version changes	224

Index 225

1

Using JP1/AO

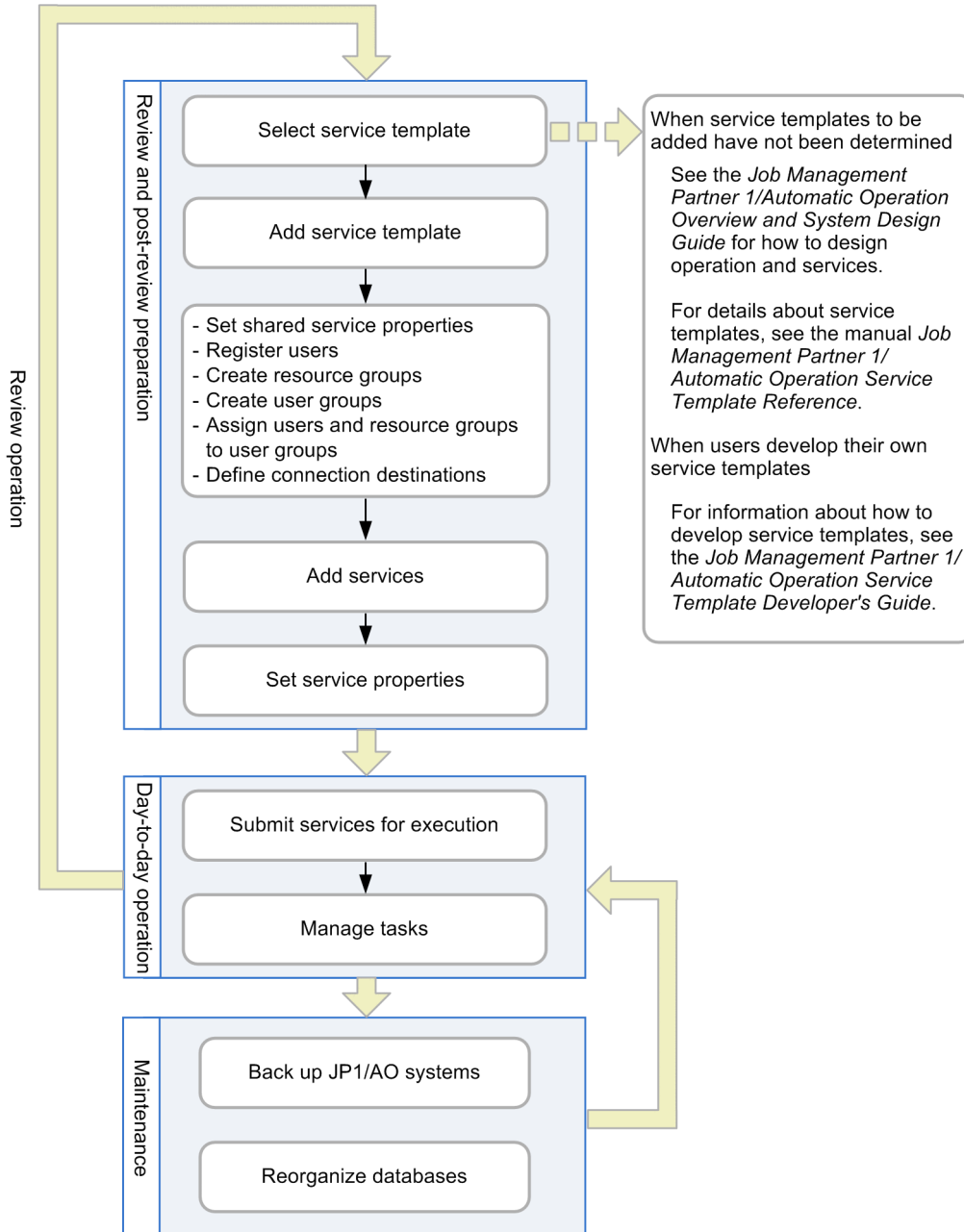
There are several phases in the operation of a JP1/AO system. The first is a preparation phase, followed by day-to-day operation, maintenance, and review phases which lead to another preparation phase. This chapter describes the tasks you need to perform in each phase, and the JP1/AO functionality used to achieve them.

1.1 Overview of JP1/AO operation

This section describes the basic steps you need to perform in each phase (preparation, day-to-day operation, maintenance, and review and post-review preparation) of JP1/AO operation.

The following figure shows the flow of JP1/AO operation.

Figure 1–1: Phases of JP1/AO system operation



1.1.1 Basic tasks in a preparation phase

After setting up a JP1/AO system, you need to prepare the system to automate the operating procedures for which the system is intended.

First, a user adds services as decided in the service and operation planning processes. At this time, the user also sets up the connection destinations, properties, users, and groups necessary to execute the services.

The following describes the basic flow of operations in the preparation phase of a JP1/AO system. The tasks in the example below are shared between two users: *User A* who is assigned the Admin role and has User Management permissions, and *User M* who is assigned the Modify role.

Tasks performed by User A (User Management permission and Admin role)

1. Select the service templates as decided in the service and operation planning processes.
2. Add the selected service templates to JP1/AO.
Add the service templates selected in the service planning process to JP1/AO.
3. Set shared service properties.
Shared service properties are properties that are shared by more than one service. Set the property value of the service share property defined for the added service template. If necessary, set the shared built-in service property.
4. Register users.
Add users who will add and execute services.
5. Create resource groups.
A resource group is a unit that groups together services and connection destinations.
6. Create user groups.
A user group is a set of users who belong to the same organization or share responsibilities.
7. Assign users and resource groups to user groups.
By allocating resource groups to user groups, you can control the access each user has to specific services. For example, you can provide services in a multi-tenant system by managing services efficiently in the context of user groups.
8. Define connection destinations.
To limit the connection-destination hosts of a service, you need to have registered the hosts as connection destinations. For connection destination definitions, set connection destination information including the host name (or IP address) of the connection destination, and the connection destination type. In addition, set authentication information, such as user IDs and passwords, as necessary.

Tasks performed by User M (Modify role)

1. Use the service templates added by User A to add services.
2. Set service properties.
Prepare services for execution by adding them to JP1/AO and setting the appropriate property values.

Related topics

- [1.3 Managing service templates](#)
- [1.4 Managing services](#)
- [1.7 Setting shared service properties](#)
- [1.10 Managing users](#)
- [1.11 Managing groups](#)

- [1.12 Managing connection destination](#)

1.1.2 Basic tasks in day-to-day operation

After adding services to JP1/AO in the preparation phase, you can execute the services that carry out the desired operating procedures. Executed services are processed as tasks, whose progress and status you can check.

The following describes the basic flow of day-to-day operations in a JP1/AO system. The tasks in the example below are shared between two users: *User S* who is assigned the Submit role, and *User M* who is assigned the Modify role.

Tasks performed by User S (Submit role)

1. Execute services.
2. Review email notifications, and deal with tasks that are waiting for a response, in an abnormal state, or have failed. If a task is waiting for a response, enter the required information in the window provided. For tasks in Abnormal Detection or Failed status, take the appropriate action to resolve the issue.
3. Check the progress and results of tasks, as needed. The user can also pause and resume scheduled and recurring tasks.

Tasks performed by User M (Modify role)

1. Periodically move tasks that no longer need monitoring from the Tasks list to the History list. Also, delete tasks histories that are no longer required from the History list.

Related topics

- [1.5 Submitting services for execution](#)
- [1.6 Managing tasks](#)
- [1.18 Email notification](#)

1.1.3 Basic tasks in maintenance phase

A JP1/AO system requires regular maintenance to assist in the reorganization of database data. You do not need operating permission for the JP1/AO system to perform maintenance.

The following describes the basic flow of maintenance tasks in a JP1/AO system.

Maintenance tasks

1. Create backup data for the JP1/AO system.
2. Reorganize the database used by the JP1/AO system.

Related topics

- [12. Maintenance](#)

1.1.4 Basic tasks in review phase and post-review preparation phase

Review JP1/AO operation when changes are made to the operating procedures you are automating, or new procedures are added. You can then add or change services and settings based on the results of the review process.

The following describes the basic flow of operations in the post-review preparation phase of a JP1/AO system. The tasks in the example below are shared between two users: *User A* who is assigned the Admin role and has User Management permission, and *User M* who is assigned the Modify role. When these operations are completed, you can resume day-to-day use of JP1/AO with the results of the review phase implemented.

Tasks performed by User A (User Management permission and Admin role)

1. Add new versions of service templates.
You can use an upgraded service template alongside an old version of the same template.
2. Other miscellaneous changes, as follows:
 - Delete old versions of service templates for which you have no further use.
 - Change the values of service share properties as needed.
 - Register or delete users as needed.
 - Create, edit, or delete resource groups as needed.
 - Create, edit, or delete user groups as needed.
 - Create, edit, or delete definitions of connection destinations as needed.

Tasks performed by User M (Modify role)

1. Add services based on the upgraded service templates.
If you elect to keep the service name used by the old version, specify the old service name as the name of the new service.
You cannot use the same service name more than once in a given resource group. If you want to keep the old version of a service, rename the old version first.
2. Set service properties.
A new service does not inherit the property values of old versions of the same service. If you want to keep the same settings as the old version, set the same values in the properties of the new service.

Related topics

- [1.3 Managing service templates](#)
- [1.4 Managing services](#)
- [1.7 Setting shared service properties](#)
- [1.10 Managing users](#)
- [1.11 Managing groups](#)
- [1.12 Managing connection destination](#)

1.2 List of JP1/AO features

JP1/AO provides a number of features in several categories. In the first category are automation features that define and execute services that automate work tasks, and in the second are resource management features that manage users, connection destinations, and other resources. The third category are features that link with other products, including email notification when errors occur, and direct access URL which lets you access a specific part of the user interface directly.

The features of JP1/AO are listed in the tables below.

For details on each feature, see the location in the Refer to column.

Table 1–1: Automation features

Feature	Description	Refer to
Service template management	Adds service templates to JP1/AO. You can also delete service templates that are no longer required, or create custom service templates.	1.3 Managing service templates
Service management	Uses service templates to add services to be executed. You can also edit added services, or delete services that are no longer required.	1.4 Managing services
Service execution	Executes services to automate work tasks. Each time a user submits a service for execution, he or she enters the required property values and specifies the execution timing. The required property values differ among services. When you execute a service, a corresponding task is generated and processing begins at the time determined by the execution timing.	1.5 Submitting services for execution
Task management	Checks the status and progress of tasks, and controls task processing. Tasks that have finished processing can be moved from the Tasks list to the History list.	1.6 Managing tasks
Setting of shared service properties	Sets shared service properties common to more than one service. You can also set the shared built-in service properties defined in advance in JP1/AO as common settings within JP1/AO.	1.7 Setting shared service properties
Setting of preset properties	Sets in a single operation a set of property values appropriate for the user environment and the mode of operation when services are added or edited.	1.8 Setting preset properties
Categories	You can categorize services and tasks by purpose, type, and other criteria, and display them in a hierarchy.	1.9 Assigning categories

Table 1–2: Resource management features

Feature	Description	Refer to
User management	Registers, edits, and deletes users who log in to JP1/AO. You can also use this feature to change user passwords and the status of user locks.	1.10 Managing users
Group management	Creates, edits, and deletes resource groups and user groups. By allocating resource groups to user groups, you can individually control the level of access each user registered in the user group has to resources. By allocating roles to resource groups, you can also control the features each user is able to use.	1.11 Managing groups

Feature	Description	Refer to
Connection destination management	Manages resources in the context of connection destinations. By registering a resource as a connection destination in JP1/AO, you can restrict access to connection destinations based on the resource group to which a task belongs.	1.12 Managing connection destination

Table 1–3: Linkage features

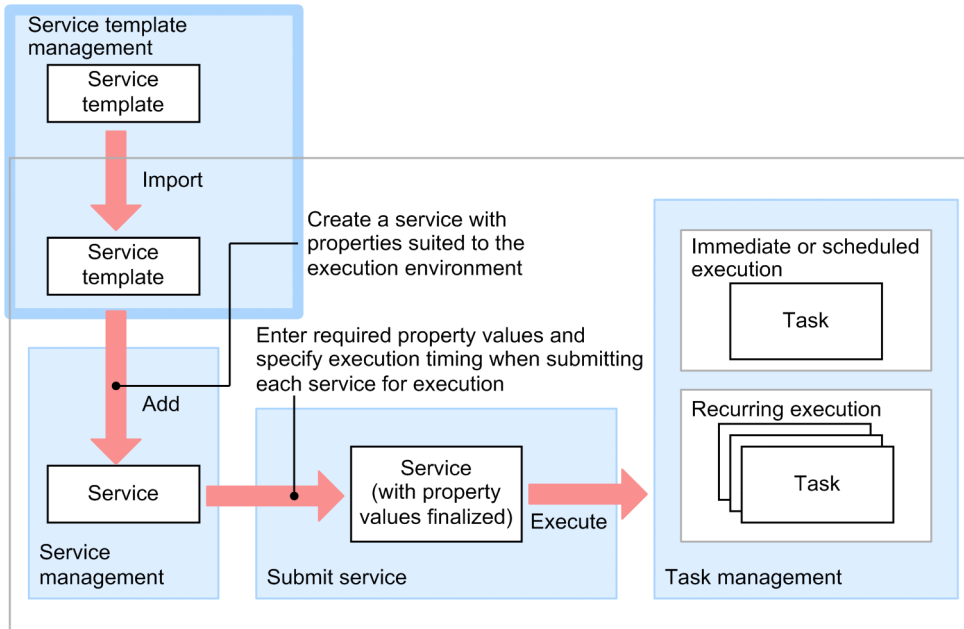
Feature	Description	Refer to
Linking with JP1/Base authentication	You can manage JP1/AO users and perform user authentication by linking with the authentication functionality of JP1/Base. Using JP1/Base authentication eliminates the need to manage users and user groups from JP1/AO. It also allows you to use the JP1 user accounts already in use with other JP1 products.	1.14 Linking with JP1/Base authentication
Linking with Active Directory	By linking with Active Directory, you can use users and groups managed by Active Directory in JP1/AO. Note that only when JP1/AO uses Active Directory as the LDAP directory server, you can link with Active Directory.	1.15 Linking with Active Directory
Linking with JP1/IM event monitoring	By linking JP1/AO with JP1/IM, you can centrally manage the JP1 events issued by JP1/AO from JP1/IM.	1.16 Linking with JP1/IM event monitoring
Linking with JP1/AJS3	By linking JP1/AO with JP1/AJS3, you can execute JP1/AO services or stop the execution of tasks from the JP1/AJS3 server.	1.17 Linking with JP1/AJS3
Email notification	This feature notifies you by email when a task fails or enters an abnormal status.	1.18 Email notification
Direct-access URL	You can display a target window immediately after you log in by specifying the URL of the window as a direct access URL.	1.19 Direct-access URLs
Link&Launch	You can launch Hitachi Command Suite products in single sign-on mode from the JP1/AO interface.	1.20 Configuring Link&Launch
Linking with business content in JP1/Integrated Management - Navigation Platform	You can open a JP1/IM - NP window in single sign-on mode from the JP1/AO interface.	1.21 Linking with JP1/IM - NP business content

1.3 Managing service templates

This functionality lets you add service templates to JP1/AO. You can also use it to delete service templates that are no longer needed and to create custom service templates.

The following figure shows the general procedure for automating operating procedures, and how it relates to service template management.

Figure 1–2: Flow of operating procedure automation (service template management)



JP1/AO server

The service template management functionality lets you perform the following tasks:

Add (import) service templates

Add service templates to JP1/AO.

When adding service templates, you can specify a zip file containing a set of service templates, or an individual service template file (*file-name.st*).

Delete service templates

Delete a service template that is no longer needed from JP1/AO.

If you have added services based on a service template, delete the service before you delete the service template.

Add preset properties

Preset properties are a collection of property values defined for a particular user environment or mode of operation. When you add or edit a service, you can use preset properties to assign values suited to the user environment or how the system is used. To assign preset properties, create a preset property definition file.

Output (export) service template lists

You can output a list of service templates to a file in CSV format. Uses for this file include as a reference for managing service templates, and to investigate which service templates need to be added to the system.

Create service templates

You can create custom service templates by copying and editing one of the standard service templates provided with JP1/AO. You can also create your own service template without using the service template provided by JP1/AO.

Note that product support applies to service templates provided with JP1/AO (JP1/AO standard-package service templates and JP1/AO Content Set), but not to edited versions of these templates. However, Hitachi will provide support for plug-ins provided by JP1/AO (JP1/AO standard-package plug-ins and JP1/AO Content Set) that are called from an edited service template.

For details about how to create a service template, see the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

Related topics

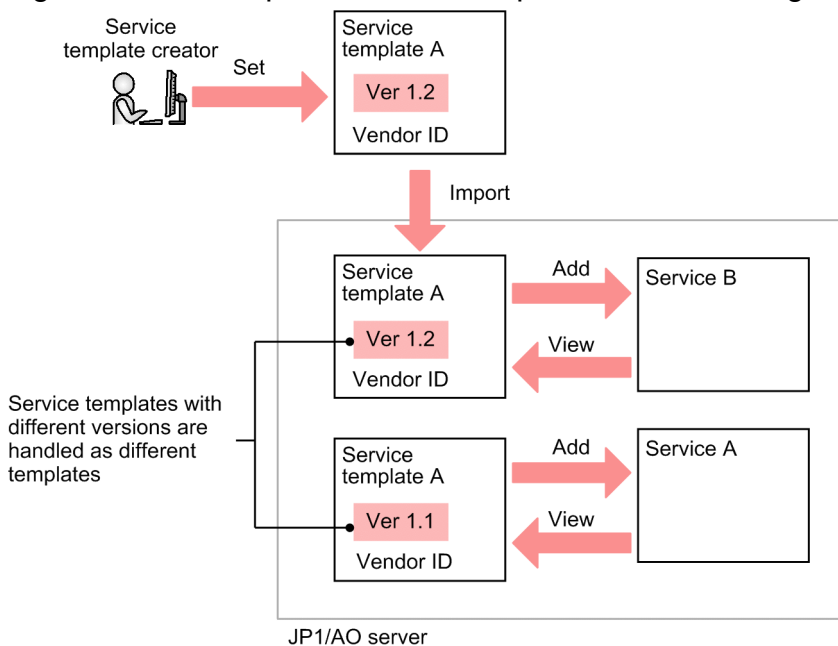
- [3.2 Adding \(importing\) a service template to JP1/AO](#)
- [3.3 Deleting service templates from JP1/AO](#)
- [3.4 Adding preset properties to service templates](#)
- [3.5 Outputting \(exporting\) service template lists](#)

1.3.1 Service template versions

Version information is defined in each service template. JP1/AO manages service templates separately if the version, vendor ID, or template name is different. This allows you to use service templates of different versions together when needed.

The following figure shows an example of how JP1/AO manages service template versions.

Figure 1–3: Example of service template version management



1.3.2 Storage location of service templates in JP1/AO standard-package plug-ins and JP1/AO Content Set

Service templates in JP1/AO standard-package plug-ins and JP1/AO Content Set are stored in the following folders:

For JP1/AO standard-package plug-ins

JP1/AO-Contents-installation-folder\contents\setup

For JP1/AO Content Set

JP1/AO-content-set-installation-folder\contents\setup

Service templates in JP1/AO standard-package plug-ins and JP1/AO Content Set are compressed in a zip file. By specifying the zip file for the `/file` option of the `importservicetemplate` command, you can use service templates in JP1/AO.

Related topics

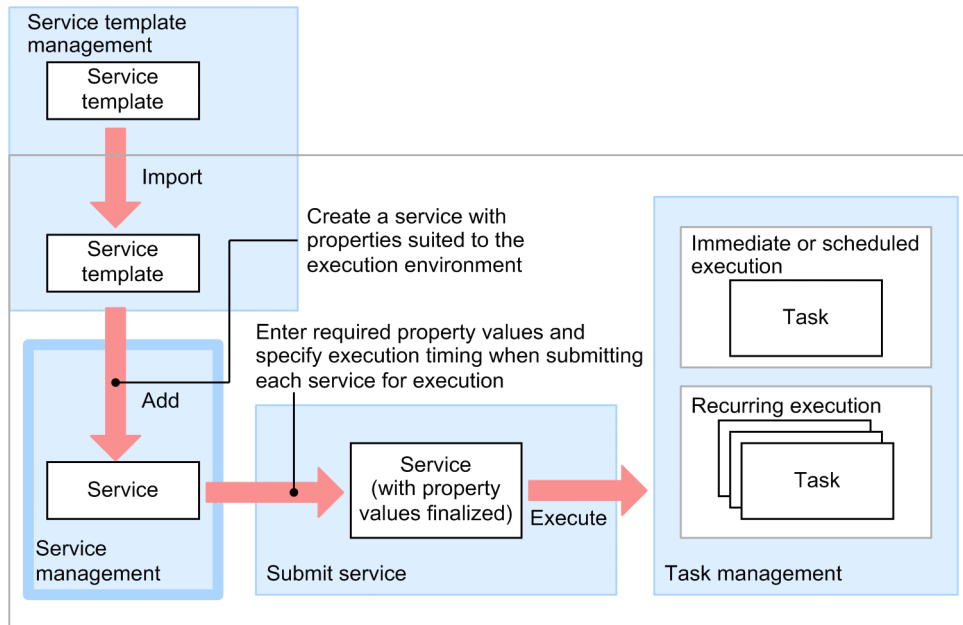
- *Installation folder for each product and JP1/AO - Contents and JP1/AO Content Set, installation folder* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

1.4 Managing services

You can add services to be executed based on service templates that have been added to JP1/AO. You can also edit a service you added, and delete services that are no longer required.

The following figure shows the general procedure for automating operating procedures, and how it relates to service management.

Figure 1–4: Flow of operating procedure automation (service management)



JP1/AO server

Service management functionality lets you perform the following tasks:

Adding services

You can add services for execution by the JP1/AO system. You add a service by entering property values in a service template.

You can add more than one service from the same service template.

Editing services

You can go back and edit the parameters you set when adding a service. However, you cannot change resource groups (groupings of services and their connection destinations) after a service has been registered. To change a resource group, you need to delete the service and then add it again.

You can edit the properties of an active service, even if there are tasks in the JP1/AO system that were generated from that service. Any changes you make do not apply to tasks that are already generated, or to existing task histories.

Deleting services

You can delete services from the JP1/AO system when they are no longer required.

You can only delete a service when there are no tasks in the JP1/AO system that were generated from that service. If such tasks exist, move them to the task history list before deleting the service. You can delete a service for which history entries exist in the history list.

Outputting (exporting) service lists

You can output a list of services to a file in CSV format. Uses for this file include as a reference for managing services, and to investigate which services are required in your system.

Related topics

- 1.10 Managing users
- 4.1 Adding services
- 4.2 Editing services
- 4.3 Deleting services
- 4.4 Outputting (exporting) a list of services

1.4.1 Intervening actions while defining services

If you are using the **Service Definition** dialog box and another user intervenes by performing an action (editing, deleting, or submitting a service) that affects the service you are using, the results of the intervening action apply.

The tables and figures below show what happens when another user performs an intervening action.

Table 1–4: Results of intervening actions when using the **Service Definition** dialog box

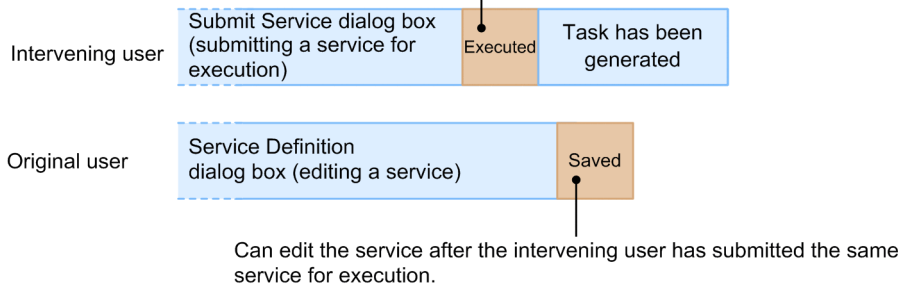
No.	Intervening action	Result of intervening action
1	Submit service	User performing intervening action This user is able to submit the service. The service submitted by the intervening user does not reflect the settings applied by the original user. User using Service Definition window This user is able to edit the service.
2	Edit service	Intervening user The user is able to edit and save the service. Original user When the user edits and saves the service, the original user's settings apply.
3	Delete service	Intervening user The user is able to delete the service. Original user The user cannot save the results of the editing process.

The following figure shows how JP1/AO behaves when an intervening action is performed in the **Service Definition** dialog box.

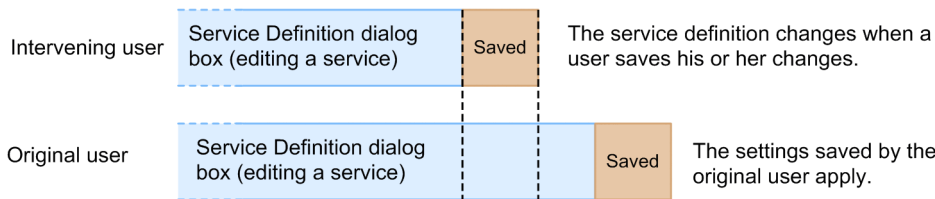
Figure 1–5: Behavior of JP1/AO when an intervening action is performed in the **Service Definition** dialog box

● If another user intervenes and submits a service for execution

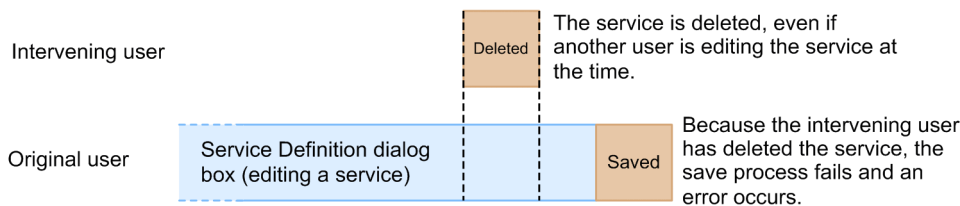
Can submit the service for execution while the original user has the service displayed in the Service Definition dialog box.



● If an intervening user edits a service



● If an intervening user deletes a service



If another user edits or executes a service that has finished executing, it will have no effect on tasks that have already been generated. If another user attempts to delete a service, he or she will be unable to delete the service if tasks generated from that service appear in the Tasks list.

1.4.2 Intervening action when submitting a service

If you are using the **Submit Service** dialog box and another user intervenes by performing an action (editing, deleting, or submitting a service) that affects the service you are using, the results of the intervening action apply.

The following table describes what happens when another user performs an intervening action.

Table 1–5: Results of intervening actions when using the **Submit Service** dialog box

No.	Intervening action	Result of intervening action
1	Submit service	Intervening user The user can submit the service for execution. Original user The user can submit the service for execution.
2	Edit service	Intervening user The user can edit and save the service.

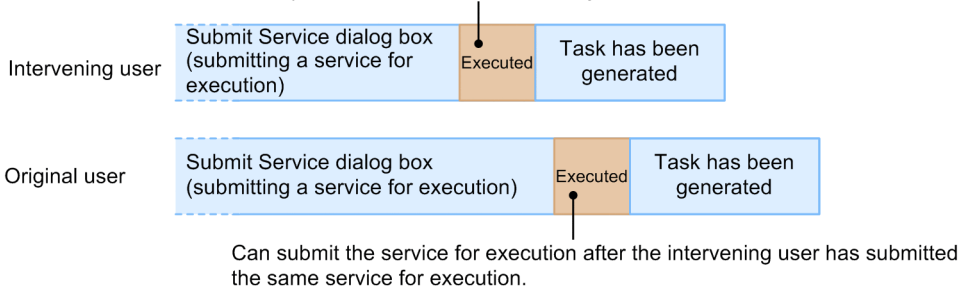
No.	Intervening action	Result of intervening action
2	Edit service	Original user The changes made by the intervening user do not appear in the Submit Service dialog box. However, the service properties edited by the intervening user in the Service Definition dialog box apply when the original user submits the service for execution.
3	Delete service	Intervening user The user can delete the service. Original user The user cannot delete the service.

The following figure shows how JP1/AO behaves when an intervening action is performed in the **Submit Service** dialog box.

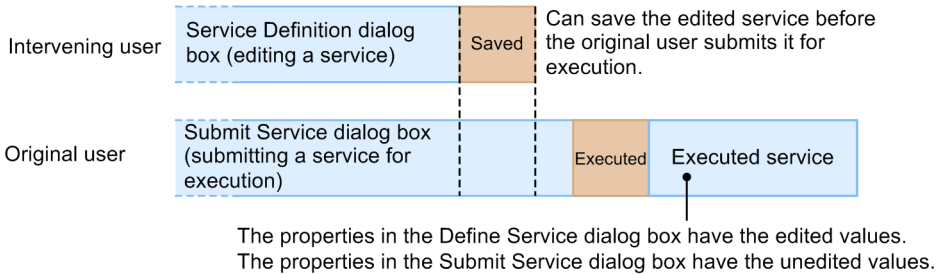
Figure 1–6: Behavior of JP1/AO when an intervening action is performed in the **Submit Service** dialog box

● If an intervening user submits a service for execution

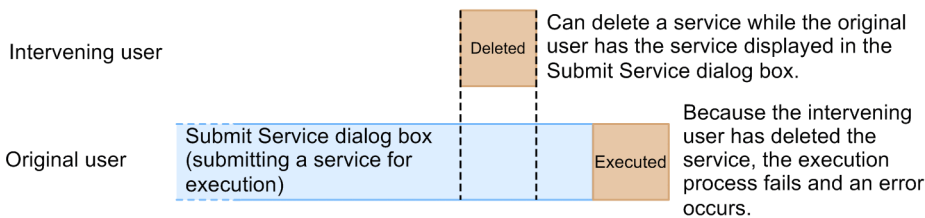
Can submit the service for execution while the original user has the service displayed in the Submit Service dialog box.



● If an intervening user edits a service



● If an intervening user deletes a service



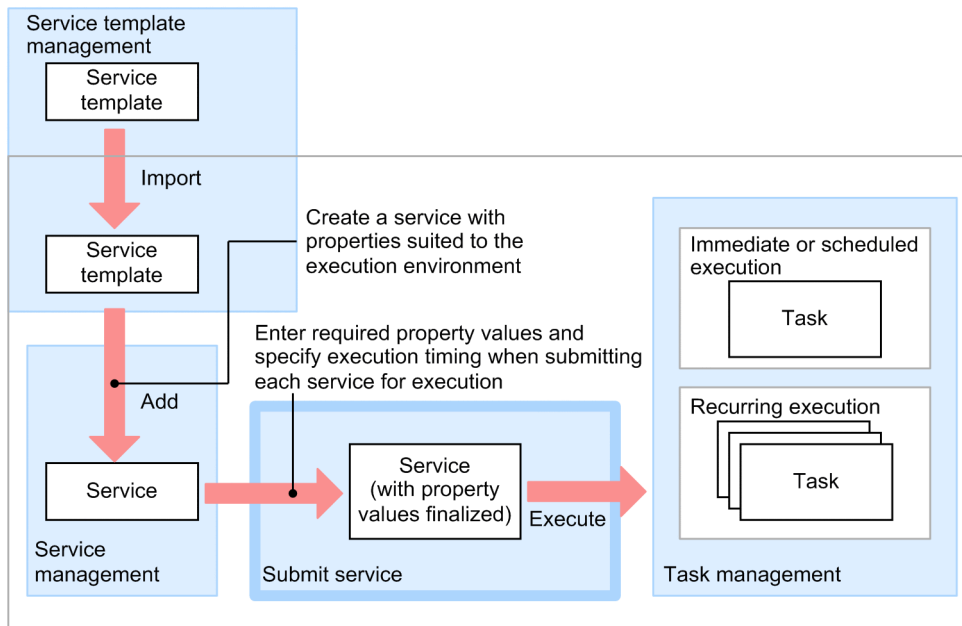
If another user edits or executes a service that has finished executing, there will be no effect on tasks that have already been generated. If another user attempts to delete a service when tasks generated from that service appear in the Tasks list, he or she will be unable to delete the service.

1.5 Submitting services for execution

By submitting services for execution, you can automate the operating procedures for which the JP1/AO system is intended. When you submit a service, you specify the required property values and the execution timing. The required property values differ among services. When you submit a service, JP1/AO generates a task associated with the service, which starts processing at the specified timing.

The following figure shows the general procedure for automating operating procedures, and how it relates to service submission.

Figure 1–7: Flow of operating procedure automation (service submission)



JP1/AO server

You can submit a service for immediate execution, scheduled execution, or recurring execution.

Immediate execution

When you submit a service, a task is generated and begins processing immediately.

Scheduled execution

When you submit a service, a task is generated and begins processing at the scheduled start time.

Recurring execution

When you submit a service, a task is generated and begins processing according to the scheduled start time and recurrence pattern.

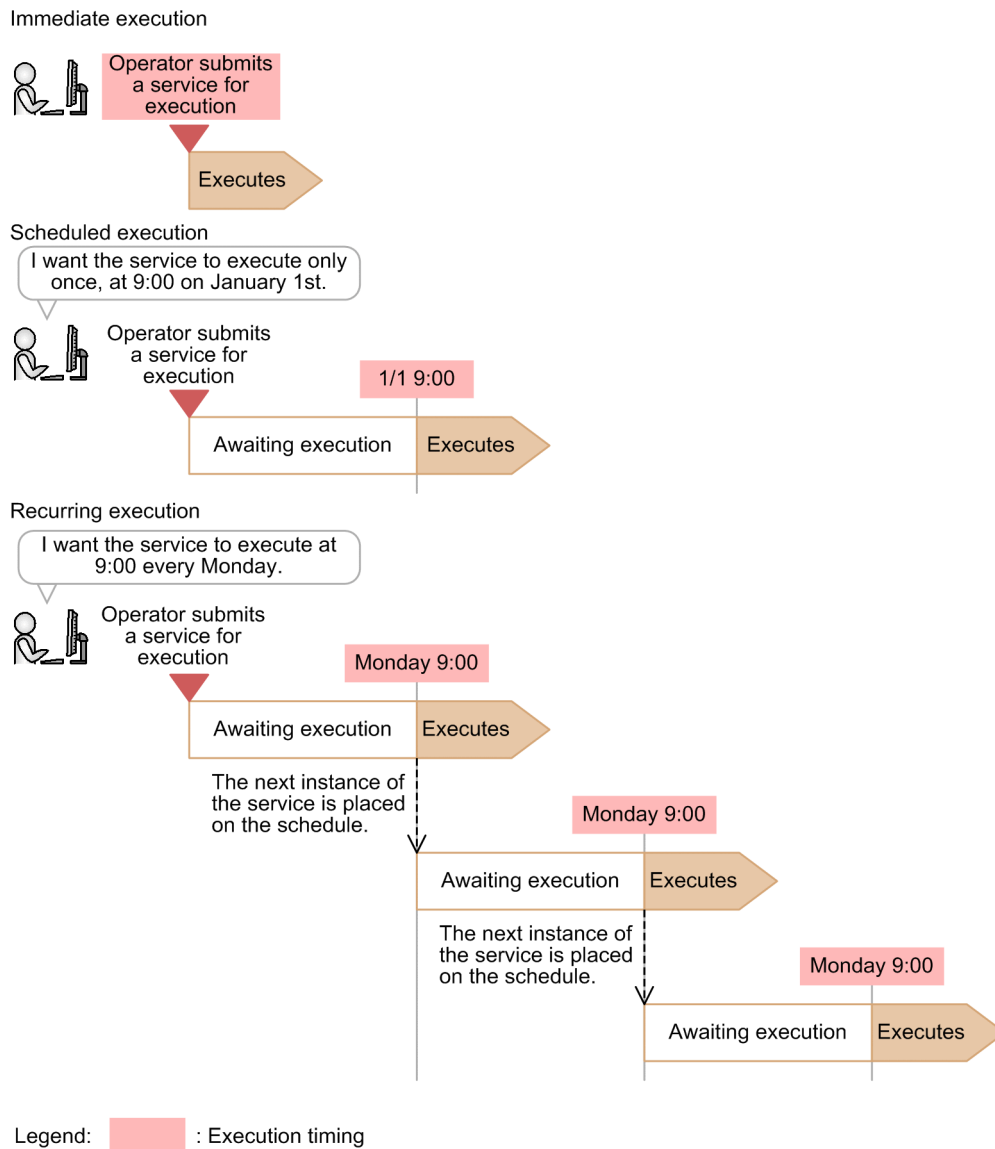
Related topics

- [5.1 Submitting services for immediate execution](#)
- [5.2 Submitting services for execution at a specified time](#)
- [5.3 Submitting services for recurring execution](#)

1.5.1 Timing of executing services

A service that is submitted for execution is processed at the specified timing. The following figure shows when services are executed when a timing is specified.

Figure 1–8: Timing of executing a service



Tasks for scheduled or recurring execution are executed when the scheduled start time arrives.

However, service execution will be delayed in the following cases:

- When the scheduled start time arrives and the previous task has not finished executing
The task will be executed when the preceding task finishes executing.
- When JP1/AO stops while the task is in Waiting status, and restarted after the scheduled start time has passed
The task will be executed after JP1/AO restarts.

If you specify an execution start date or time that has already passed, an error occurs.

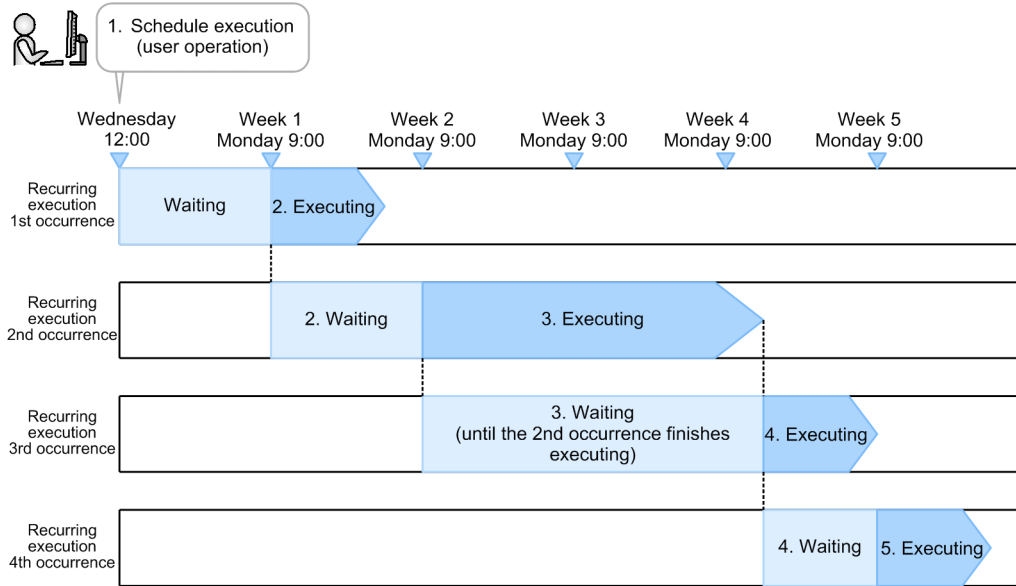
1.5.2 Process of recurring execution

If you specify recurring execution as the execution timing for a service, the JP1/AO system generates the first task as soon as you submit the service. JP1/AO executes the first task when the scheduled start time arrives, at which point a second task is generated. The process of executing and generating tasks continues on an ongoing basis according to the schedule (time and frequency) specified for the service.

Generated tasks remain in Waiting status until they begin executing.

Note that processing might be delayed if the preceding task has not finished when the next execution start time arrives. The following figure shows an example of a service scheduled for recurring execution at 9:00 every Monday.

Figure 1–9: Example of recurring execution



1. Service submitted by user (at 12:00 on Wednesday)

A user submits a service with recurring specified as the execution timing, and an execution schedule of 9:00 every Monday. At this point, JP1/AO generates the first task.

2. First recurring execution (at 9:00 on Monday of week 1)

JP1/AO executes the first task at the scheduled start time, and generates the second task.

3. Second recurring execution (at 9:00 on Monday of week 2)

JP1/AO executes the second task as scheduled (as determined from the time and frequency), and generates the third task.

4. Third recurring execution (at 9:00 on Monday of week 3)

If the second task has not finished by the next scheduled start time, JP1/AO executes the third task when the second task finishes. At this time, the fourth task is also generated.

5. Fourth recurring execution (at 9:00 on Monday of week 4)

JP1/AO executes the fourth task at the first occurrence of the scheduled start time (as determined from the time and frequency) after the fourth task is generated. At this time, the fifth task is also generated.

The process of executing and generating tasks continues in this manner.

You cannot change the schedule after you submit a service. To change the schedule of a service, stop any generated tasks and then re-submit the service with the new schedule.

1.5.3 Using JP1/AO in time zones affected by daylight saving

When you use JP1/AO in a time zone where daylight saving time applies, the following start times are affected:

- Start times of services submitted for scheduled execution
- Start times of services submitted for recurring execution

The explanation below uses the example of Central Daylight Time (USA and Canada). The start and end times for CDT are as follows:

- Start of daylight saving
2:00:00 on second Sunday in March
- End of daylight saving
2:00:00 on first Sunday in November

(1) Switching from standard time to daylight saving time

The timing with which tasks start after the system switches from standard time to daylight saving time is determined from the start time set for the task, and the time difference between standard and daylight saving time. At 2:00:00 on the second Sunday in March, the clock switches to 3:00:00. This means that the period from 2:00:00 to 2:59:59 standard time is skipped over. If you set up a task to start within this period, it will start at 3:00:00 daylight saving time.

If you set it up to start at 3:00:00 or later standard time, the task will start at 3:00:00 or later after the transition to daylight saving time has taken place. This means that the task will start, in relative terms, one hour ahead of its scheduled start time.

The following table shows how tasks are scheduled around the transition from standard time to daylight saving time.

Table 1–6: Scheduling at the transition from standard time to daylight saving time

Start time setting	1:59:59 or earlier	2:00:00 to 2:59:59	3:00:00 or later
Actual start time	Executed at 1:59:59 or earlier standard time	Executed at 3:00:00 daylight saving time	Executed at 3:00:00 or later daylight saving time

(2) Switching from daylight saving time to standard time

The timing with which tasks start after the system switches from daylight saving time to standard time is determined from the start time set for the task, and the time difference between standard and daylight saving time. When the time reaches 2:00:00 on the first Sunday of November, the clock switches to 1:00:00 standard time. The result is an extra hour in standard time, from 1:00:00 to 2:00:00. Tasks that were scheduled to start between 1:00:00 and 1:59:59 are started at the scheduled time in daylight saving time, and are not started again after the transition to standard time.

If you set up a task to start at 2:00:00 daylight saving time or later, it will start at 2:00:00 in standard time, after the transition to standard time has taken place. This means that the task will start, in relative terms, one hour later than its scheduled start time.

The following table shows how tasks are scheduled around the transition from daylight saving time to standard time.

Table 1–7: Scheduling at the transition from daylight saving time to standard time

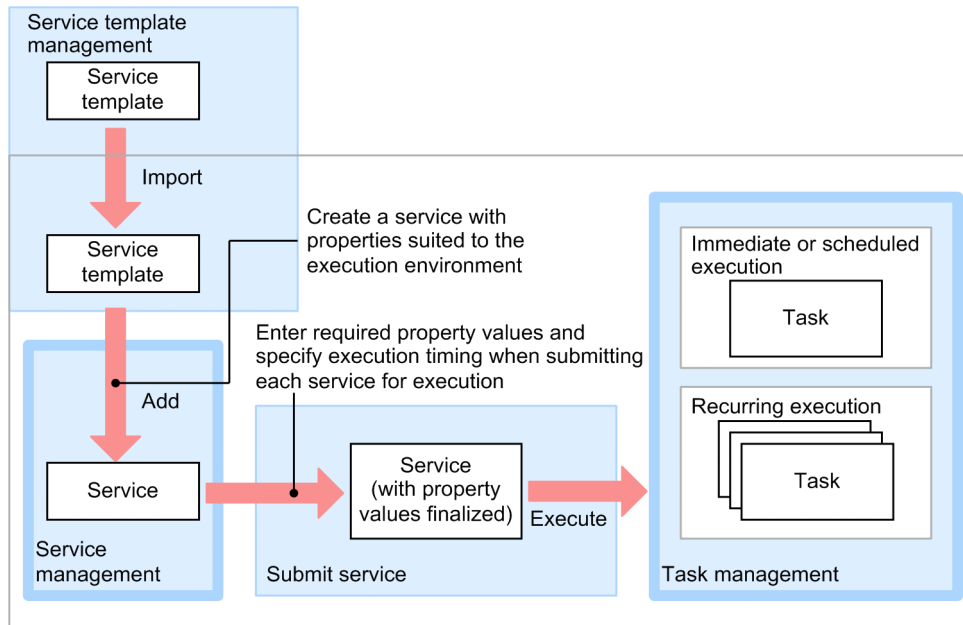
Start time setting	0:59:59 or earlier	1:00:00 to 1:59:59	2:00:00 or later
Actual start time	Executed at 0:59:59 or earlier daylight saving time	Executed between 1:00:00 and 1:59:59 daylight saving time	Executed at 2:00:00 or later standard time

1.6 Managing tasks

Task management functionality lets you check the status and progress of tasks, and control task processing.

The following figure shows the general procedure for automating operating procedures, and how it relates to task management.

Figure 1–10: Flow of operating procedure automation (task management)



JP1/AO server

Tasks that have finished processing can be moved from the Tasks list to the History list in a process called *archiving*. Archiving can be performed manually or automatically. Older task histories moved to the History list can be deleted manually or automatically.

The task management function lets you perform the following tasks:

Tip

For task management you perform in the **Tasks** window, you can also perform the following operations for debug tasks:

- Managing task progress
- Stopping tasks
- Stopping tasks forcibly

For details about how to perform debug tasks, see the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

Check the progress of tasks

You can check the status of executed tasks and the processing status. Statuses include the In Progress and Completed statuses, and are updated as tasks are processed.

In the task summary area, you can check the status of the tasks executed by a logged-in user, the status of all tasks in a list, and the progress of a task. You can also check the progress of the flow of the task you selected in the **Task Monitor** view.

Enter actions for tasks waiting for a response (Enter a response)

You can enter a response when a task requires input from a user.

When a task requires a user to make a decision or selection, it enters Waiting for Response status. You can identify tasks in this status by checking the task summary or tasks list.

When a task enters Waiting for Response status, the appropriate user is notified by email. The email notification feature requires you to specify SMTP server settings, user IDs, and other information. By linking with JP1/IM, you can issue JP1 events reporting that a task has entered Waiting for Response status.

Manage schedules

You can suspend, resume, or cancel waiting or held tasks. You can manage the schedules of only waiting and held tasks. If you want to stop the execution of a task that has already executed, you must perform the processing that stops task execution.

Stop tasks

You can stop a task that is in progress.

When you stop a task, steps that are executing continue processing. Steps that have not started executing yet are not processed. At that time, the task enters the Failed or Completed status. Note that if you stop the task when the window for entering responses is displayed, the user-response operation ends in an error.

Forcibly stop

You can forcibly stop a task that is in progress.

When you forcibly stop a task, the task stops without waiting for steps in progress to be completed. At that time, the task enters the Failed or Completed status. The execution result of a plug-in is not applied to the value of the service property.

If a plug-in that is in progress is a content plug-in, the process tree that is being executed in the target device is forcibly stopped immediately, and the execution result of commands are not guaranteed. For details about operations when the plug-in that is in progress is a basic plug-in, see the related topics section for each basic plug-in in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

Note that if you forcibly stop tasks that are executed regularly, there will be no influence on the next execution.

Resubmit tasks

Tasks that have stopped processing (tasks in the Completed, Failed, or Canceled status) can be executed as a different task with another task ID.

Note that JP1/AO sets Immediate as the execution timing for resubmitted tasks. Change the execution timing as needed.

Retry

You can retry a failed step, or the step after the failed one.

You can retry a task with the same property value and with the same task ID. After retrying a task, you can check the history of the retried tasks in the task log and the public log.

Move (archive) tasks

You can move finished tasks whose results you have checked to the History list.

Tasks moved to the History list can be viewed regardless of category. This allows you to view in a list all tasks that have finished processing.

Tasks are set to be moved regularly to the History list in JP1/AO.

Delete histories

You can delete histories that are no longer require management.

Note that histories are set to be deleted regularly in JP1/AO.

Output (export) task lists

You can output task lists and task histories to a CSV file. You can then use this file to gather and analyze statistics, or use it as a record.

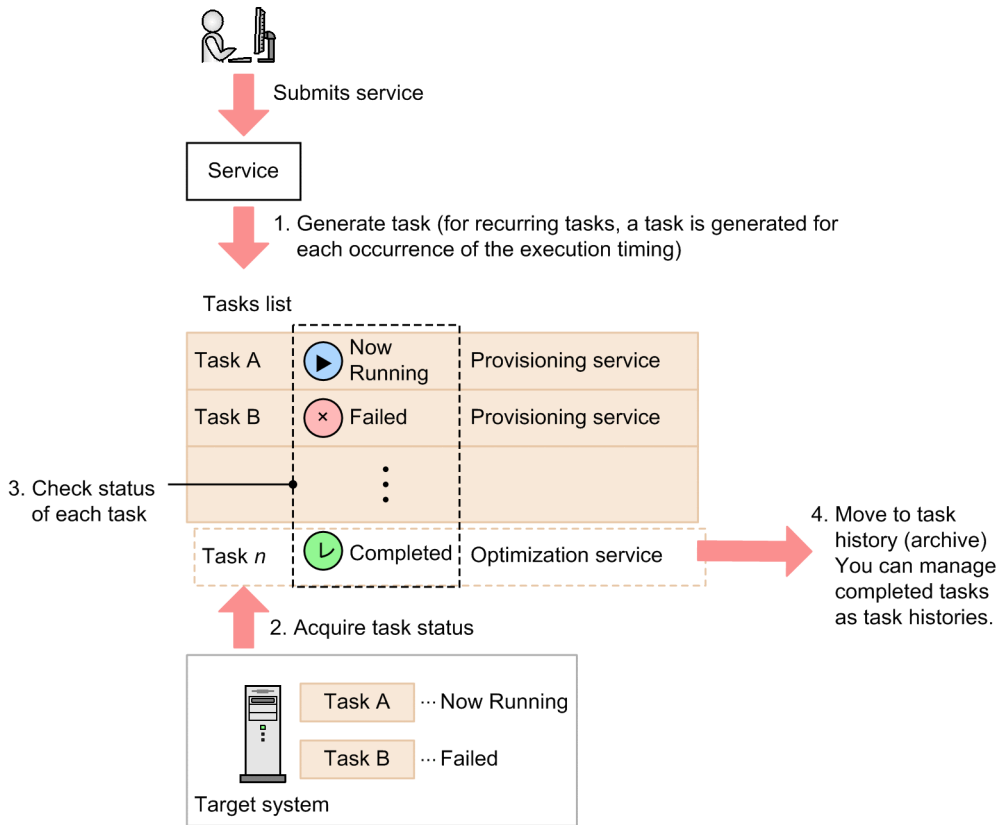
Related topics

- [6.1 Checking the status of tasks executed by the logged-in user](#)
- [6.2 Checking the status of all tasks](#)
- [6.3 Checking the progress of a task](#)
- [6.6 Entering actions for tasks waiting for a response \(entering responses\)](#)
- [6.7 Suspending tasks \(suspending schedules\)](#)
- [6.8 Resuming suspended tasks \(resuming schedules\)](#)
- [6.9 Canceling tasks \(canceling schedules\)](#)
- [6.10 Stopping tasks \(execution stop\)](#)
- [6.11 Redoing tasks](#)
- [6.12 Moving tasks to the History list \(archiving tasks\)](#)
- [6.13 Deleting task histories](#)
- [6.14 Outputting task lists \(exporting tasks\)](#)

1.6.1 Overview of task management

The following figure provides an overview of task management.

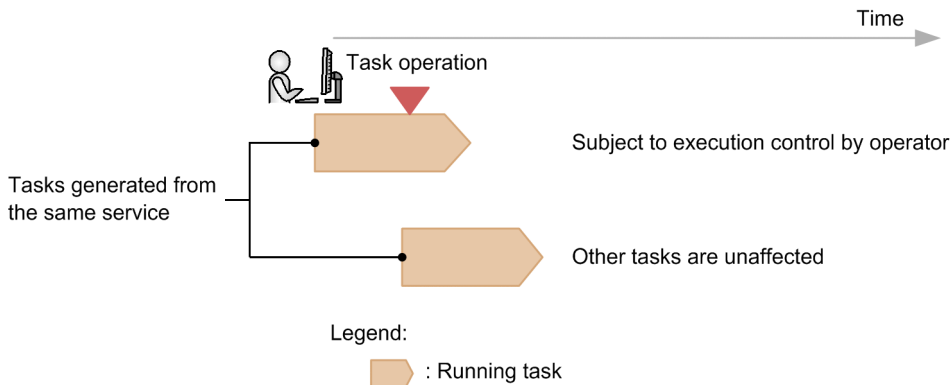
Figure 1–11: Overview of task management



1. When a user submits a service for execution, JP1/AO generates a task.
2. JP1/AO acquires the status of the task from the system where the operation is being performed, and displays it in the Tasks list.
3. The user monitors the processing status of tasks.
If necessary, the user can stop a task or provide a response for a task that enters Waiting for Response status.
4. JP1/AO automatically moves tasks that have exceeded the retention period to the History list. This processing can also be done manually.

Processing performed for a task affects only the task for which the processing is performed. Tasks generated from the same service are not affected.

Figure 1–12: Effects on task operations



1.6.2 Managing schedules

You can suspend waiting tasks or resume held tasks. You can also cancel waiting or held tasks.

Suspend tasks

You can suspend waiting tasks that are executed at a specific time or on a recurring basis.

The execution of the tasks and the generation of subsequent tasks are held until the schedule is resumed.

Resume schedules

You can resume schedules that have been suspended.

When you resume a schedule, tasks that were being held become executable again (they enter Waiting status) and are executed at the scheduled start time. If you resume a schedule after the scheduled start time, the task is executed immediately.

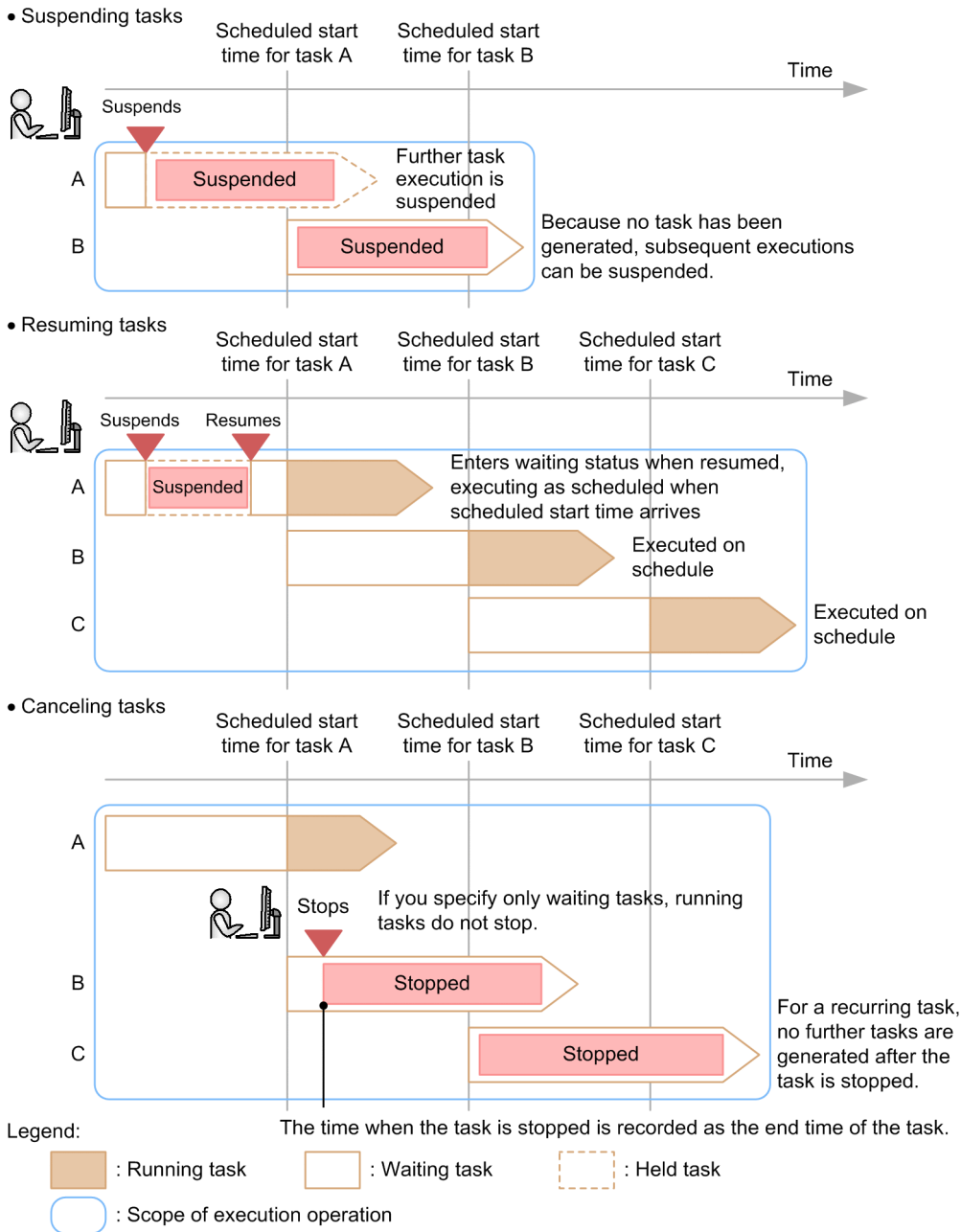
Cancel schedules

You can cancel waiting or held tasks that are executed at specific dates and times as well as waiting tasks that are executed on a recurring basis. When you do so, the execution of the tasks and the generation of subsequent tasks are canceled.

If you suspend or cancel schedules of waiting tasks that are executed on a recurring basis, subsequent tasks are not generated while the schedule is suspended. When the schedule resumes, the tasks are executed at the scheduled start date and time.

The following figure shows the behavior when the schedule of a waiting task that is executed on a recurring basis is suspended, resumed, or canceled.

Figure 1–13: Suspending and resuming tasks



1.6.3 Managing task progress

You can check the progress of tasks according to user need by using any of the following methods:

Checking the status of tasks executed by a logged-in user

You can check the status of tasks executed by a logged-in user for each of the statuses in the task summary area.

You can also display a list of tasks that have the applicable status in the task summary area in order to check details or take action.

Checking the statuses of all tasks

You can check in a list the statuses of all tasks that can be viewed by users.

By checking the task statuses such as In Progress or Completed in the task list, you can get a good understanding of how tasks are being processed automatically.

The list also shows when tasks start and finish processing, who submitted tasks, and other information.

Checking the progress of a task

You can check the progress of a task being processed by JP1/AO.

You can also find out how far the processing of a task has progressed, which plug-in the task is currently processing, and other information.

(1) Overall progress of a task

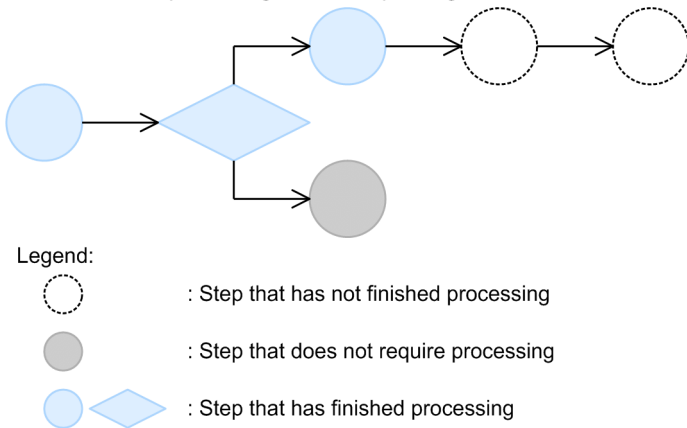
In the detailed task information, the progress of the highest level of the task flow is displayed as follows:

(number-of-steps-that-have-finished-processing + number-of-steps-that-do-not-require-processing) / number-of-all-steps-contained-in-the-flow

The following figure shows an example of a task flow.

Figure 1–14: Example of task progress

Structure of the processing flow corresponding to the task



JP1/AO calculates the progress of the processing flow as follows:

$$\text{Progress} = (3+1)/6$$

$$= 4/6$$

(2) Progress of individual task components

As detailed task information, JP1/AO displays the status, return value, start time, end time, and comment for each step name. The status in the detailed task information indicates the step status, or the status in the task processing engine.

You can change information displayed in the status by using the property file (config_user.properties). By default, the status of the step is displayed.

The following table describes information that is displayed as step statuses.

Table 1–8: Step statuses and corresponding processing status categories

No.	Step status	Processing status category
1	Waiting	Steps that have not finished processing

No.	Step status	Processing status category
2	Interrupted	Steps that have not finished processing
3	Interrupted (After Execution)	
4	In Progress	
5	Waiting for Response	
6	Abnormal Detection	
7	Not Executed	
8	Failed	
9	Bypassed	
10	Completed	Steps that have finished processing
11	Ended with a Warning	
12	Waiting to Repeat	Out of scope [#]

#

Indicates the status before steps under the Repeated Execution Plug-in or repeated execution flows enter the repeated execution status. Therefore, the status is not displayed for the top flow.

The following table describes information that is displayed as statuses in the task processing engine.

Table 1–9: Task processing engine statuses and corresponding processing status categories

No.	Task processing engine status	Processing status category
1	Not sched. to exe.	Steps that have not finished processing
2	Wait for start time	
3	Waiting for prev. to end	
4	Waiting to execute	
5	Now queuing	
6	Shutdown	
7	Now running	
8	Failed to start	
9	Failed to start - WR	
10	Killed	
11	Killed - WR	
12	Not executed + Ended	
13	Not executed + Ended - W	
14	Running + Abend	
15	Running + Warning	
16	Ended abnormally	
17	Ended abnormally - WR	

No.	Task processing engine status	Processing status category
18	Unknown end status	Steps that have not finished processing
19	Unknown end status - WR	
20	Invalid exe. seq.	
21	Interrupted	
22	Bypassed	Steps that do not require processing
23	Ended normally	Steps that have finished processing
24	Normal end + False	
25	Ended with warning	

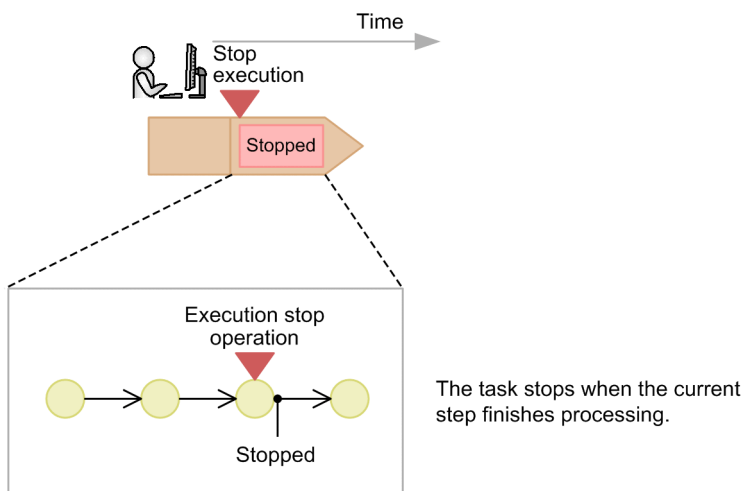
Related topics

- *Property file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*



1.6.4 Behavior when tasks are stopped

If you stop a task that is being executed, the task stops when all executing steps have finished.

Figure 1–15: Stopping tasks



Legend:

 : Executing task  : Step

Note that when you use User-Response Wait Plug-ins or Repeated Execution Plug-ins, you must take different actions if you stop a task.

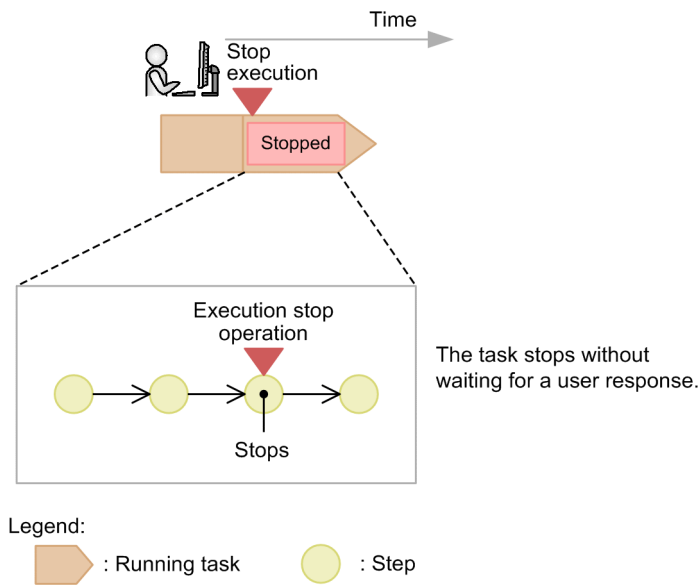
Related topics

- [1.6.5 Behavior when tasks waiting for a response have stopped](#)
- [1.6.6 Behavior when a task has stopped while repeated execution plug-ins are running](#)

1.6.5 Behavior when tasks waiting for a response have stopped

When you stop a task in the Waiting for Response status, the task stops without waiting for a response from the user.

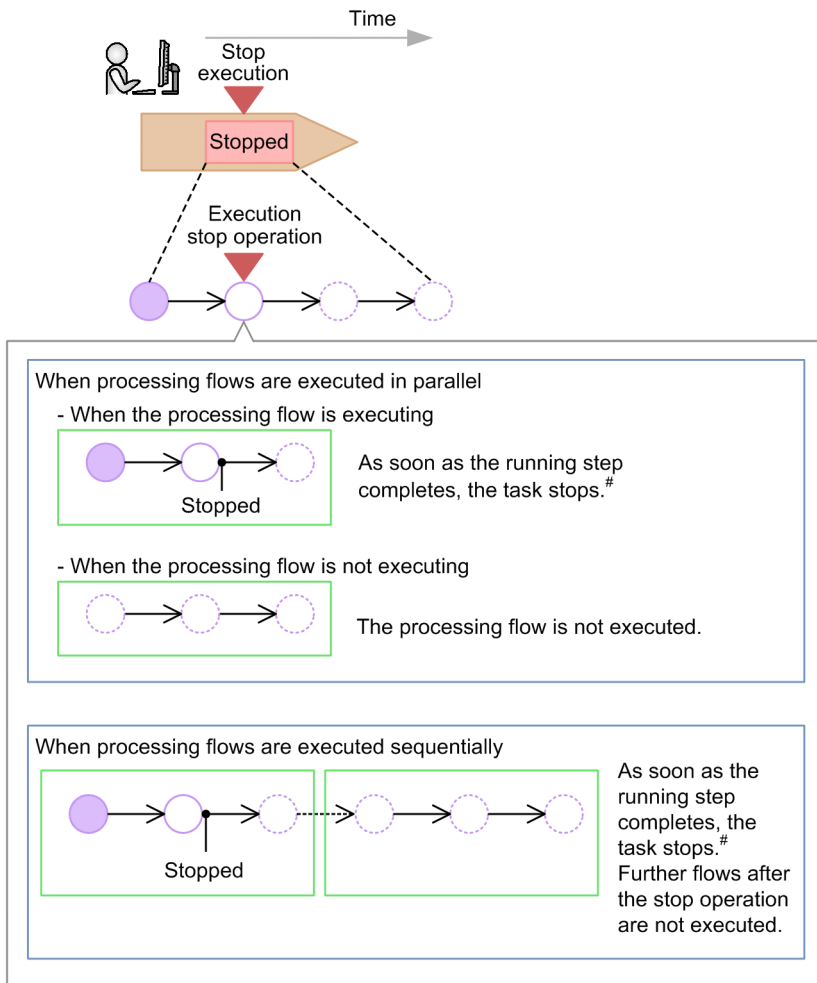
Figure 1–16: Stopping tasks in Waiting for Response status



1.6.6 Behavior when a task has stopped while repeated execution plug-ins are running

If you stop the execution of a task while executing a repeated execution plug-in, the executing step sequence stops when the executing steps finish executing. Step sequences that have not been executed are not executed.

Figure 1–17: Stopping running repeated execution plug-ins



Legend:

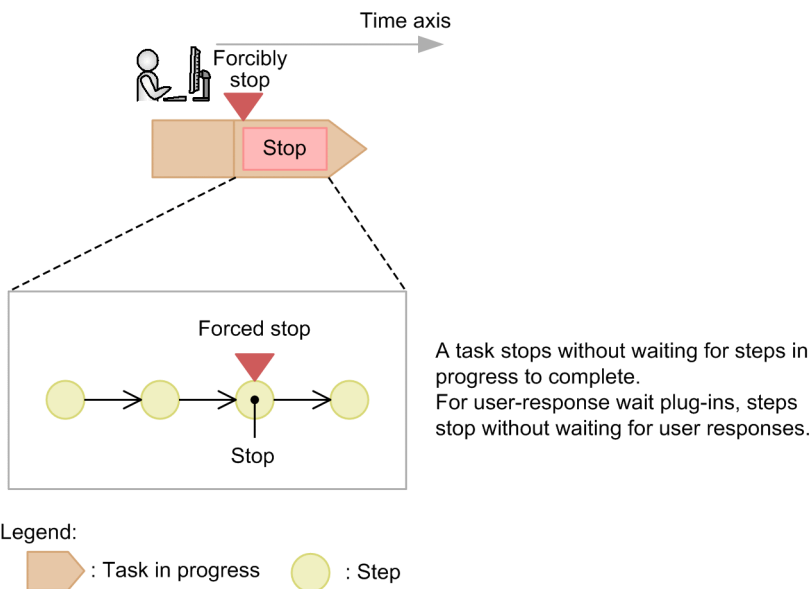
- : Executing task
- : Processing flow
- : Executed steps
- : Executing steps
- : Unexecuted steps

#: Steps for user-response wait plug-ins stop without waiting for responses from the user.

1.6.7 Behavior when a task is forcibly stopped

If you forcibly stop the execution of a task, the executing step sequence stops without waiting for executing steps to finish.

Figure 1–18: Stopping tasks forcibly



1.6.8 Retrying tasks

You can retry a failed step within a failed task, or a step after the failed step. You can retry the step with the inherited property value and the same task ID. Note that the following value is applied to the service share property:

- For the service share property, the property value used when the service was executed for the first time is applied.
- For the shared built-in service property, the property value set when the step was retried is applied.

In addition, the execution timing is *Immediate*.

Important note

If there is no failed step in a task, and the task is restored by using the `restoresystem` command, you cannot retry steps.

Updating task information by retrying steps

Data that is not updated

Task ID, task name, task description, input property, execution timing, and start time

Data to be updated

End time

The end time is updated when a retried task finishes.

Retry possibilities depending on task statuses

Depending on the status of the ended task or step, retry possibilities vary. The following examples explain whether the task or step can be retried according to the task or step status:

When a task failed in a step that does not contain the Repeated Execution Plug-in

When a task is retried, if you select **Retry the Task From the Step After the Failed Step**, the failed step ends normally, and the step after the failed one is executed.

When a task failed in a step that contains the Repeated Execution Plug-in

When a task is retried, if you select **Retry the Task From the Failed Step**, the first and the subsequent steps of the Repeated Execution Plug-in are retried.

If you select **Retry the Task From the Step After the Failed Step**, the next and the subsequent steps of the Repeated Execution Plug-in are retried. The steps of the Repeated Execution Plug-in terminate normally, but the statuses of the steps that were already executed under the Repeated Execution Plug-in remain the same.

In addition, depending on whether the condition for executing subsequent steps is set for the Repeated Execution Plug-in step, if a step under the Repeated Execution Plug-in fails, the status of the Repeated Execution Plug-in step might be Completed. In this case, you cannot retry the step of the Repeated Execution Plug-in.

When a step ended with a warning, and a task failed

Because there is no failed step, you cannot retry steps.

When the last step of a task failed

When you retry a task, if you select **Retry the Task From the Step After the Failed Step**, the failed last step ends normally. In this case, the task also ends normally, and you cannot retry steps.

Sessions when a task is retried

When a process fails in a subsequent step of the terminal connect plug-in, a session to the terminal connection destination is disconnected when the task ends. Because of this, if you retry the task, processing of the terminal command plug-in fails. In this case, re-execute the task without retrying it.

Note that when the same repeated execution flow has the terminal connect plug-in and the terminal command plug-in, if you retry from the Repeated Execution Plug-in, the repeated execution flow is retried from the beginning. Therefore, the session is reconnected. As a result, the terminal command plug-in is executed while the session remains connected.

Related topics

- [1.6 Managing tasks](#)
- [6.11 Redoing tasks](#)

1.6.9 Archiving tasks and removing histories automatically

JP1/AO archives and deletes tasks and histories automatically.

Archiving tasks automatically

Once a day, JP1/AO archives processed tasks that satisfy the following criteria in the following order:

1. Tasks whose retention period has expired
2. Tasks exceeding the maximum number of tasks that can be retained

Tasks exceeding the maximum number of tasks that can be retained are archived starting from the task that has the oldest end date and time.

Note that the maximum number of tasks that can be retained include the number of debug tasks.

You can change the retention period and maximum number of tasks that can be retained in the properties file (`config_user.properties`).

The tasks moved to the History list can be displayed regardless of category. Therefore, you can view all tasks that have finished processing in a list.

Tip

Debug tasks are deleted automatically when tasks are archived automatically. For details about deleting debug tasks automatically, see Procedure for checking the status of all debug tasks in the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

Deleting histories automatically

Histories that satisfy the criteria are deleted automatically.

Histories exceeding the maximum number of histories that can be retained are removed once a day. Deletion starts from the task that has the oldest archive date and time.

You can change the maximum number of histories that can be retained in the properties file (`config_user.properties`).

Related topics

- *Properties file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.6.10 Display format of task summary

The task summary area displays the number of tasks of each status that were generated from services submitted for execution by the user. This functionality summarizes the tasks in the Tasks list. Tasks in the History list, and debug tasks are not counted.

The task summary functionality counts tasks in each of 5 categories: In Progress, Waiting for Response, Waiting, Completed, and Failed. To see which tasks are in each status, click the *status-name* in the task summary area. Canceled tasks are not counted.

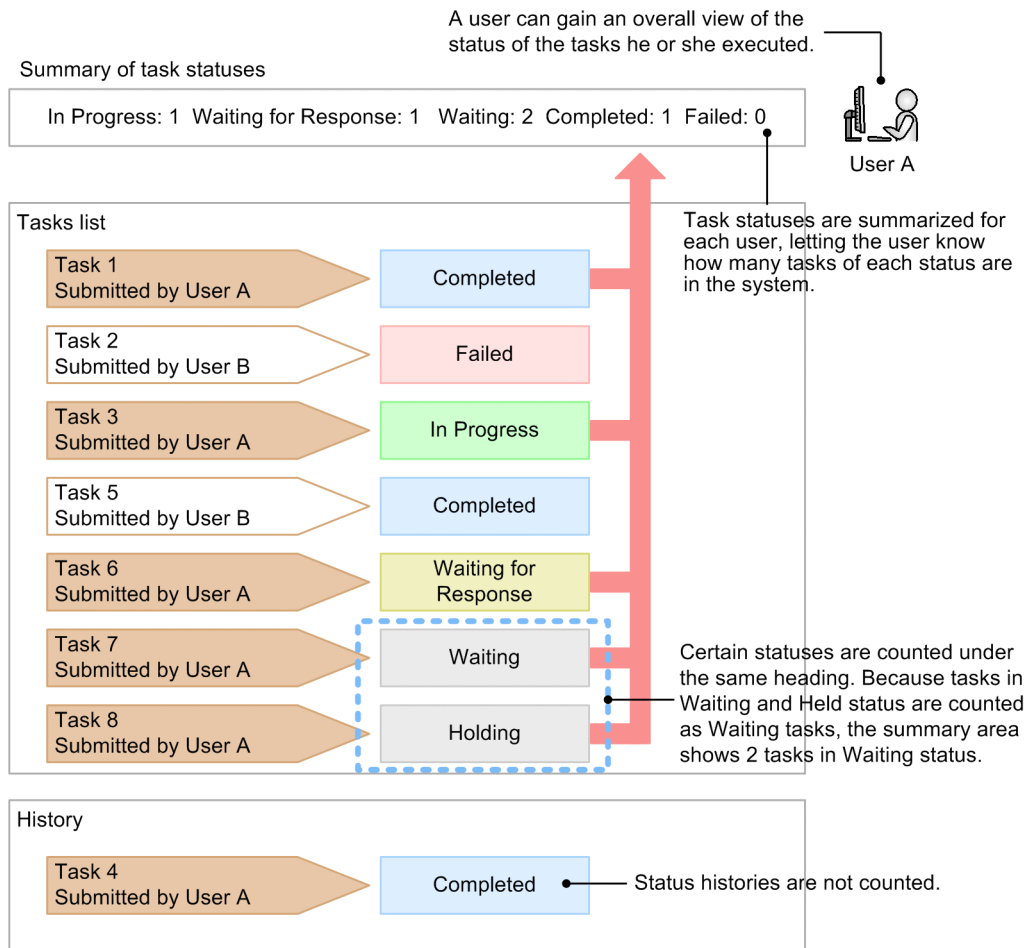
The following table shows the scope of each category in the task summary area.

Table 1–10: Scope of status categories in task summary area

No.	Status in task summary	Scope of task status
1	In Progress	In Progress, Abnormal Detection, Terminated
2	Waiting for Response	Waiting for Response
3	Waiting	Holding, Waiting
4	Completed	Completed
5	Failed	Failed

The following figure shows how task statuses are summarized.

Figure 1–19: Task summarization in task summary area



1.6.11 Task categories and generation timing

Tasks can be categorized as follows according to the execution timing specified when the task was submitted for execution.

Table 1–11: Task categories

No.	Task category	Description
1	Immediate	This category of task is generated when a user submits a service for immediate execution. When the service is submitted, the JP1/AO system generates a single task and executes it immediately.
2	Scheduled	This category of task is generated when a user submits a service for execution at a specified date and time. When the service is submitted, the JP1/AO system generates a single task and executes it once at the specified time. Between generation and execution, a scheduled task stays in Waiting status.
3	Recurring	This category of task is generated when a user submits a service for execution on a recurring schedule. When the service is submitted, the JP1/AO system initially generates a single task, and executes it at the specified time. As soon as the first task is executed, JP1/AO generates the next task which it executes based on the recurring schedule. This cycle of execution and generation is repeated on an ongoing basis. Between generation and execution, a recurring task stays in Waiting status.

The following table shows the timing with which tasks are generated.

Table 1–12: Task generation timing

No.	Service execution timing	Generated task	Task generation timing	Description
1	Immediate	Immediate execution	When the service is submitted	The task is generated when the user submits the service for execution.
2	Scheduled	Scheduled execution		
3	Recurring	Recurring execution (First task)		
4		Recurring execution (Next task)	When the task is executed	JP1/AO generates the next task when it executes the first task. The cycle of executing a task and then generating the next task continues based on the recurring schedule, until canceled by a user.

1.6.12 Task statuses and status transitions

The following table lists the task statuses used in a JP1/AO system.

Table 1–13: Task statuses

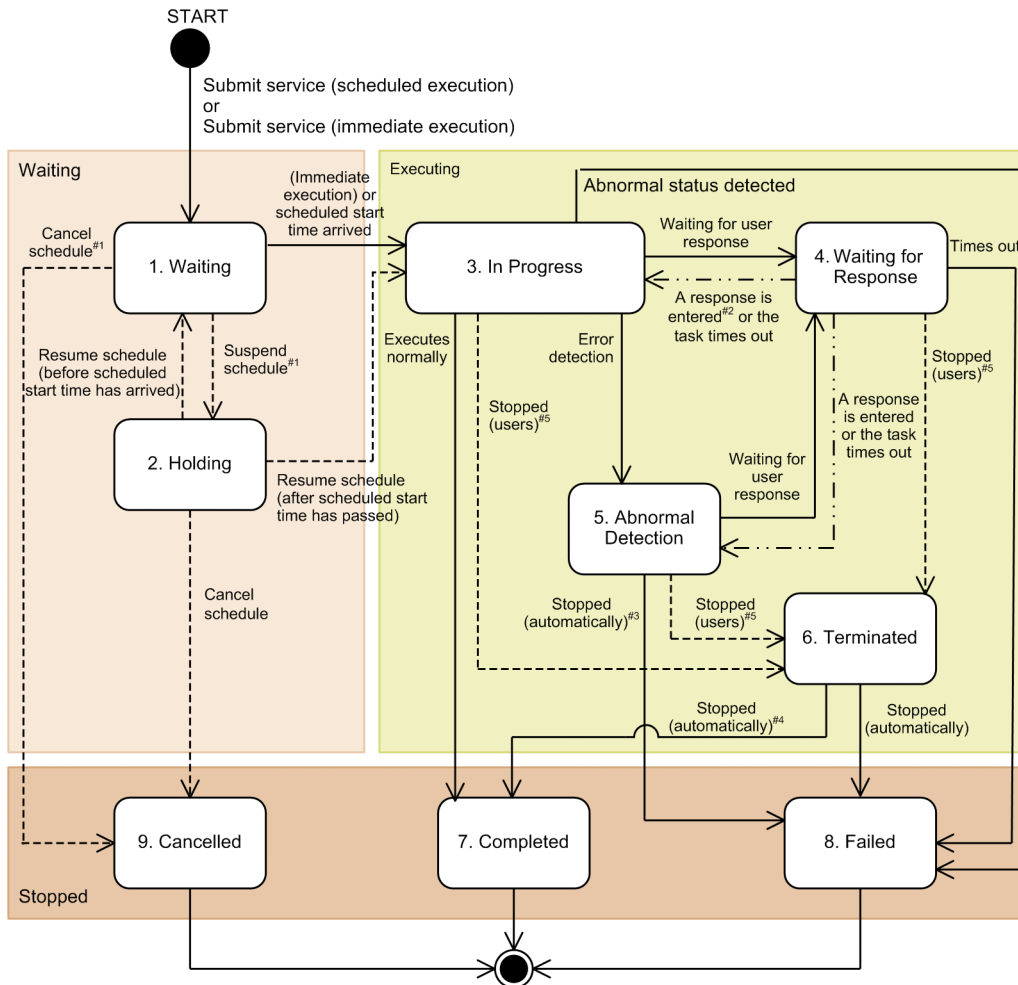
No.	Category	Task status	Description
1	Waiting	Waiting	This status applies to: <ul style="list-style-type: none"> • Tasks that are generated but have not started executing • Recurring tasks in the interval after one task finishes and before the next begins
2		Holding	This status applies to recurring tasks that have been suspended.
3	Running	Now running	This status indicates that the automated process corresponding to the task is running.
4		Waiting for Response	This status applies to tasks whose corresponding automated process requires a response from a user.
5		Abnormal Detection	This status indicates that an error has been detected in the automated process corresponding to the task.
6		Stopped	This status indicates that a user has stopped execution of or forcibly stopped the task, and JP1/AO is in the process of stopping the corresponding automated processes.
7	Stopped	Completed	Indicates that the corresponding automated process has finished normally.
8		Failed	Indicates that the corresponding automated process has not finished normally. A failure occurs when: <ul style="list-style-type: none"> • A task times out while waiting for a response • The automated process corresponding to a task stops because an error occurred[#] • JP1/AO has stopped a task in response to a stop request from a user

No.	Category	Task status	Description
8	Stopped	Failed	<ul style="list-style-type: none"> JP1/AO has stopped a task in response to the forced stop operation by a user
9		Canceled	Indicates that a user has canceled the task schedule, preventing a scheduled or recurring task from being executed.

If a user stops a task while its final plug-in is being executed, the task ends normally.

The following figure illustrates the transitions between task statuses. The labels in the figure correspond to the numbers in the Task statuses table.

Figure 1–20: Task status transitions



Legend: —>: Automatic transition - - - ->: Manual transition - · - ·>: Automatic or manual transition

- #1 This transition does not take place for tasks scheduled for immediate execution.
- #2 If the task is waiting for several responses, the transition takes place when all responses have been entered.
- #3 If the user does not intervene when the task enters Abnormal Detection status, the task enters Failed status rather than Terminated.
- #4 If the user stops the task while the final plug-in is being executed, the task transitions to Completed status.
- #5 If the user stopped operation or performed forced stop, the task enters Terminated status.

Because JP1/AO acquires task statuses at fixed intervals, the user interface might skip a number of status transitions.

For the transitions between task statuses after restoration, see [1.13.1 Notes on backup and restoration](#).

For the transitions between task statuses when JP1/AO restarts services, see [1.13.2 Notes on restarting JP1/AO services](#).

1.6.13 Step statuses

In the **Task Monitor** view, you can visually check how far steps of the running task in a flow have been processed. The following table describes information that is displayed as step statuses.

Table 1–14: Step statuses and their descriptions

No.	Category	Step status	Description
1	Waiting	Waiting	This status applies to: <ul style="list-style-type: none"> • Tasks that are generated but have not started executing • Waiting for the previous step to finish
2		Waiting to Repeat	This status indicates that steps or repeated execution flows under the recurring plug-ins are waiting for the next execution. For example, this status applies to the following cases: <ul style="list-style-type: none"> • Before a recurring plug-in is executed • When a step for a recurring plug-in is skipped by the debugger function • When a task stops before a recurring plug-in • Waiting status when a step exceeding the maximum number of steps that can be executed concurrently^{#1} is executed during recurring execution
3	Running	Interrupted	Indicates one of the following statuses: <ul style="list-style-type: none"> • Interrupted immediately before processing of a plug-in starts • Interrupted immediately after processing of a plug-in ends
4		Now Running	Indicates that the plug-in is being processed.
5		Waiting for Response	Indicates that the processing of a plug-in requires a user response.
6		Abnormal Detection	Processing of some plug-ins detects an error, but the subsequent steps are in progress.
7	Stopped	Completed	Indicates that the corresponding step has finished normally.
8		Failed	Indicates that the corresponding step has not finished normally. For example, a failure occurs when: <ul style="list-style-type: none"> • The corresponding step was stopped because it detected an error. • A user stopped a task, and the stop processing is completed. • A return value is judged to have ended abnormally with the condition for executing subsequent steps.
9		Ended with a Warning	Indicates that the corresponding step detected a warning and stopped due to subsequent execution conditions.
10		Not Executed	Indicates that the corresponding step has not been executed. ^{#2}
11		Bypassed	Indicates that the corresponding step was not executed because a plug-in did not branch off.

#1

Specify the maximum number of steps that can be executed concurrently during recurring execution in the property file (config_user.properties).

#2

Exclude steps that were not executed because a flow was branched in the judge return code plug-in or judge value plug-in.

Note that depending on the step status or plug-in type, some step statuses might not be displayed. The following table shows the step statuses and the display of each step.

Table 1–15: Step statuses and display of each step

No.	Category	Step status	Layering step (flow plug-in)	Repeated step	Repeated execution flow	Normal step
1	Waiting	Waiting	Y	Y	Y	Y
2		Waiting to Repeat	Y#	N	Y	Y#
3	Running	Interrupted	N	Y	N	Y
4		Now Running	Y	Y	Y	Y
5		Waiting for Response	N	N	N	Y
6		Abnormal Detection	Y	N	Y	N
7	Stopped	Completed	Y	Y	Y	Y
8		Failed	Y	Y	Y	Y
9		Ended with a Warning	Y	Y	Y	Y
10		Not Executed	Y	Y	Y	Y
11		Bypassed	Y	Y	N	Y

Legend:

Y: Displayed, N: Not displayed

#

If the step is under a repeated execution plug-in, the step enters Waiting to Repeat status.

Related topics

- *Property file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.6.14 Maximum number of plug-ins contained in a task that can be executed concurrently

There is a limit on the number of plug-ins (contained in a task) that can be executed concurrently in a JPI/AO system. The upper limit for normal tasks is 10, for debug tasks is 10, and they are managed separately. If you execute plug-ins exceeding the limit, they are retained in the status prior to their execution, until the currently running plug-ins finish.

Operations of the retained plug-ins are as follows:

- The step enters In Progress status.
- The start date and time of the step are set. But processing of the plug-in does not begin.

- For debug tasks, when you perform debugging, if you select **Interrupt After Each Step** for Interruption Settings, the status does not switch from In Progress to Interrupted. This is because steps are retained before they enter Interrupted status.
- A message indicating the start of plug-in execution is not output to the task log. This is because plug-ins are retained before the message is output.

To check if plug-ins are retained due to the maximum number of plug-ins that can be executed concurrently, count the number of running plug-ins to make sure plug-ins exceeding the limit are not executed. You can check the number of running plug-ins by counting them in the task list of the **Task Monitor** view, or in the debug task list.

1.6.15 Retention periods for task histories

The retention period for task histories is determined from the maximum retention count and the number of tasks generated per day. Because the JP1/AO system deletes task histories in excess of the maximum retention count, use the `listtasks` command as needed to export the History list. You can set the maximum retention count for task histories in a property file.

You can use the following method to calculate the number of days of task histories to keep:

number-of-days-of-task-histories-to-keep (truncate after the decimal point) = maximum-number-of-task-histories-to-keep / number-of-tasks-generated-per-day

Related topics

- [6.14 Outputting task lists \(exporting tasks\)](#)
- *Properties file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

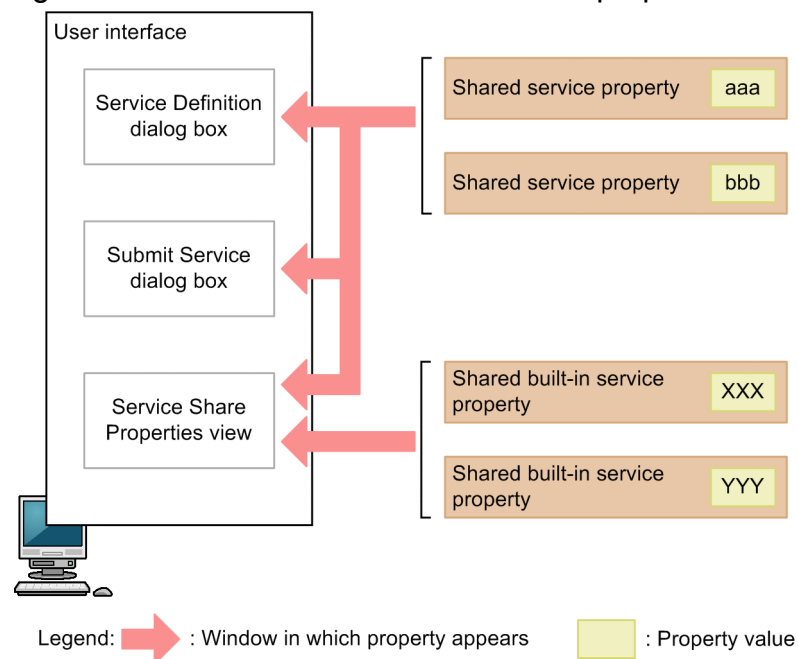
1.7 Setting shared service properties

Shared service properties are properties that are shared by more than one service.

For example, when you use a group of service templates whose common objective is to manage a particular server, you can define the host name, user ID, and password of that server in service share properties. This prevents you from having to enter the same server information each time you submit a service for execution.

There are two types of shared service properties: ordinary shared service properties associated with specific service templates, and shared built-in service properties defined in advance in JP1/AO.

Figure 1–21: Overview of shared service properties



Shared service properties

When you import a service template, the shared service properties are added to the list in the **Service Share Properties** view, and are deleted when the service template is deleted.

The parameters and default values in shared service properties depend on the service template.

You can set the parameters and default values arbitrarily when you create the service template.

Shared service properties also appear in the **Service Definition** and the **Submit Service** dialog boxes, where permitted by user permissions and the service template settings.

Shared built-in service properties

Shared service properties defined in JP1/AO in advance are called shared built-in service properties.

Shared built-in service properties appear in the **Service Share Properties** view of the JP1/AO interface after you install JP1/AO. You can set the property values arbitrarily. Because shared built-in service properties apply system-wide, they do not appear in the **Service Definition** and **Submit Service** dialog boxes for individual services.

Related topics

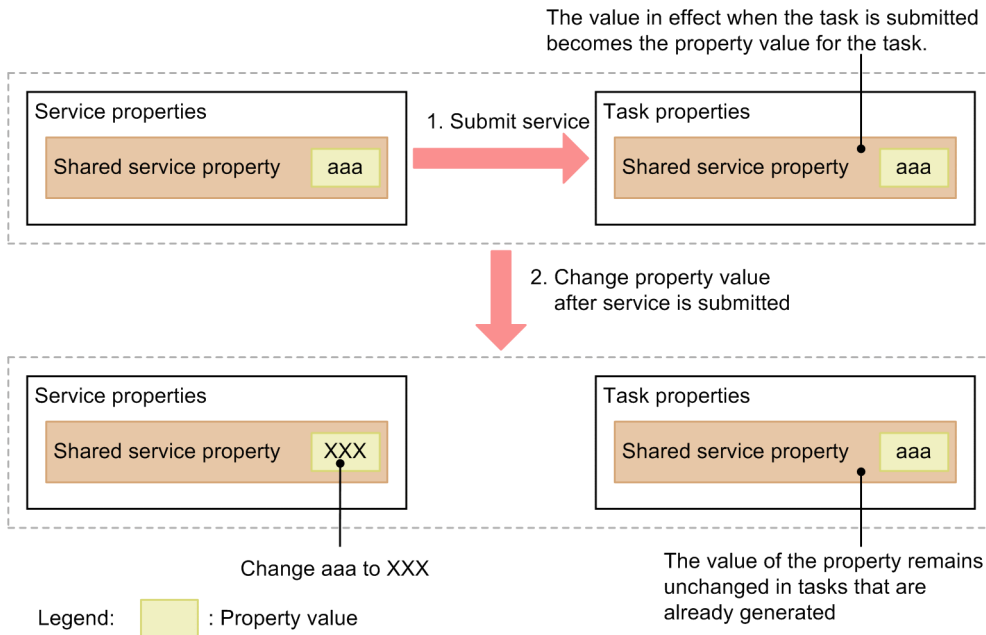
- [7.1 Procedure for setting service share properties](#)

1.7.1 Notes on setting shared service properties

Only users in the Admin role or the Develop role can set the property values for shared service properties in the **Service Share Properties** view.

When you set the value of a shared service property, the setting takes effect when the service is submitted for execution (when JP1/AO generates the task). Changes made to a property value in the **Service Share Properties** view or another window do not affect services that have already been submitted for execution. Property values set in the **Submit Service** dialog box only apply to tasks generated from that service. If you want the new value to apply to services that are already submitted, stop the service and submit it again.

Figure 1–22: Changing shared service property values after submitting a service



If you change the value of a shared built-in service property after submitting a service for execution, the change applies when the system references the property. For example, if you change the recipient (TO) of notification emails after submitting a service, the new setting applies the next time the JP1/AO system sends a notification email.

In a service template, you can define a shared service property that uses the same key name as a shared built-in service property. In this case, changes to the shared service property take effect when the service is submitted.

1.7.2 List of shared built-in service properties

The following shared built-in service properties are defined in advance, and can be used as common properties in a JP1/AO system.

Table 1–16: Shared built-in service properties

Item	Description	Required	Property key name#1
Email notification function ON/OFF	Turns the email notification function on (true) or off (false). The default is false (off).	Yes	com.hitachi.software.dna.sys.mail.notify

1. Using JP1/AO

Item	Description	Required	Property key name ^{#1}
SMTP server address	Specifies the address of the SMTP server. You can specify a host name or an IP address in IPv4 or IPv6 format.	--	com.hitachi.software.dna.sys.mail.smtp.server
SMTP server port number	Specifies the port number of the SMTP server. The default is 25.	--	com.hitachi.software.dna.sys.mail.smtp.port
SMTP server user ID	Specifies the user ID of the user account for logging in to the SMTP server. Specify domain user accounts in one of the following formats: <ul style="list-style-type: none"> <i>domain-name\user-name</i> <i>user-name@domain-name</i> 	--	com.hitachi.software.dna.sys.mail.smtp.userid
SMTP server password	Specifies the password of the user account for logging in to the SMTP server.	--	com.hitachi.software.dna.sys.mail.smtp.password
Notification email sender	Specifies the sender of notification emails.	--	com.hitachi.software.dna.sys.mail.from
Notification email recipients (TO) ^{#2}	Specifies the recipients (TO field) of notification emails. You can specify multiple email addresses separated with commas.	--	com.hitachi.software.dna.sys.mail.to
Notification email recipients (CC) ^{#2}	Specifies the recipients (CC field) of notification emails. You can specify multiple email addresses separated with commas.	--	com.hitachi.software.dna.sys.mail.cc
Notification email recipients (BCC) ^{#2}	Specifies the recipients (BCC field) of notification emails. You can specify multiple email addresses separated with commas.	--	com.hitachi.software.dna.sys.mail.bcc
JP1 user name ^{#3}	Specifies the JP1 user who submits the service. The default is the value specified by the user at installation.	Yes	com.hitachi.software.dna.sys.jp1.username
JP1 user password ^{#3}	Specifies the password of the JP1 user who submits the service. The default is the value specified by the user at installation.	Yes	com.hitachi.software.dna.sys.jp1.password
Task logging level	Specifies the logging level for tasks. The default is 10.	Yes	com.hitachi.software.dna.sys.task.log.level
Pass phrase of the private key (for SSH public key authentication)	Specifies the passphrase for the private key when using the public key authentication for SSH connection.	--	com.hitachi.software.dna.sys.ssh.privatekey.passphrase

Legend:

Yes: Indicates a mandatory property. --: Indicates an optional property.

#1

At JP1/AO installation, services are not automatically able to reference shared built-in service properties. To allow services to reference a shared built-in service property, specify the property key of the desired shared built-in service property as the service property when you create the service template.

#2

Make sure the email addresses you specify are valid. If even one address is invalid, the notification email will not be sent to any recipients.

1. Using JP1/AO

#3

Specify the account information for a JP1 user who meets both of the following criteria:

- The user has JP1_AJS_Manager or JP1_JPQ_Admin permission for resource group *.
- The user is mapped to an OS user with Administrators permission.

Related topics

- [13.9.3 Task log details](#)

1.8 Setting preset properties

1.8.1 About preset property definition files

Preset property definition files define beforehand the values used to set the properties that appear in the **Service Definition** dialog box. You can use a preset property definition file to set property values appropriate for the user environment and mode of operation in a single operation after importing service templates into a JP1/AO system.

To add a service template, you must enter values appropriate for the user environment and mode of operation for multiple properties. The preset property definition file lets you set the values for the properties that appear in the **Service Definition** dialog box in a single operation. We recommend that you define property values in a preset property definition file when you want to set values appropriate for the user environment and mode of operation all at once.

You can set the maximum number of preset properties that can be added to a single service template in the property file (config_user.properties). If you want to store multiple preset property definition files, use unique preset names in one service template.

Related topics

- [1.8.2 Preset property definition file format](#)
- [3.4 Adding preset properties to service templates](#)

1.8.2 Preset property definition file format

Define the preset property definition file as follows:

- The definition format is *property-key = property-value*.
- Use UTF-8 character encoding.
- A line starting with the hash mark (#) is a comment line.
- Characters are case sensitive.
- Blank lines are ignored.

How to write a property key

- For *property-key*, specify the property key that is defined as the input property in the **Edit Service Definition** dialog box. Note that you can define only property keys for which you want to set values.
- Specify only one property key and setting value on each line.
- If you specify multiple definitions for the same property key, the last entered definition is used.
- Characters from the first character to the character that precedes the equal sign (=) on each line of the preset property definition file are treated as a property key.

How to write a property value

- For *property-value*, specify a value meeting the criteria specified for **Data Type**, **Minimum Length**, **Maximum Length**, and **Restricted Character** in the **Edit Service Definition** dialog box.
- All characters on a line after the equal sign (=) in the preset property definition file are treated as a property value
- If you do not want to specify a property value, use the format *property-key = linefeed*.

In the following cases, if you select a preset name and click the **Apply** button in the **Service Definition** dialog box, an error occurs.

- The preset property definition file is larger than 1 MB.
- A property key that is not an input property was entered.
- A property key that is not defined in the **Edit Service Definition** dialog box was entered.
- A property key with `date` specified for **Data Type** in the **Edit Service Definition** dialog box was entered.
- The preset property definition file name is invalid.

For details about file name formats and specifiable characters, see [3.4 Adding preset properties to service templates](#).

1.9 Assigning categories

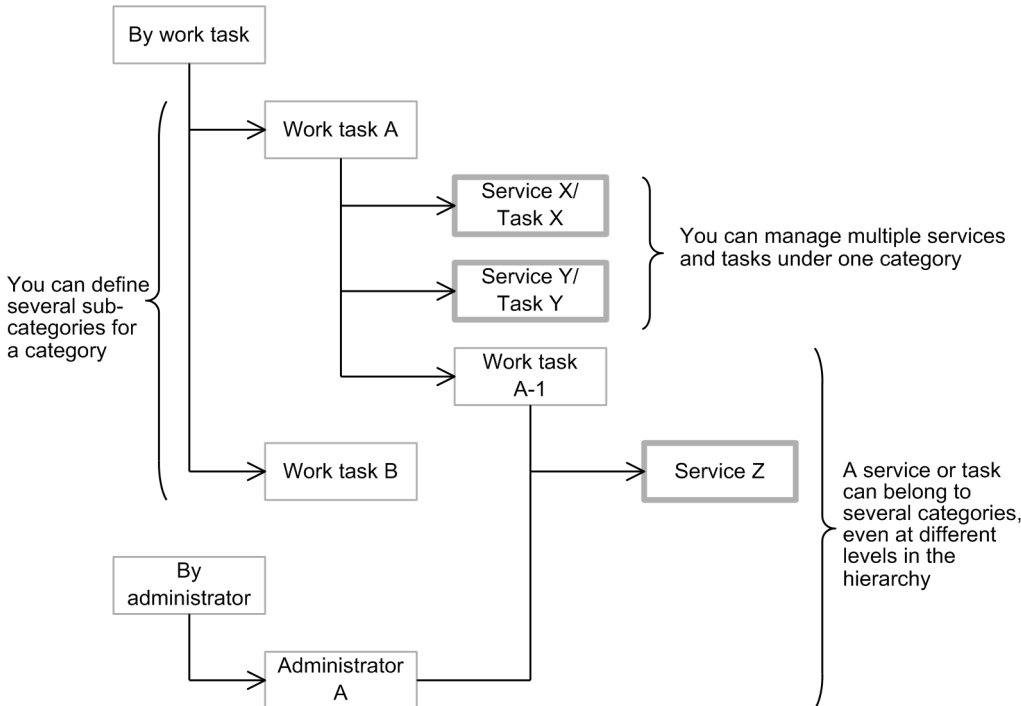
You can categorize services and tasks by purpose, type, and other criteria, and display them in a hierarchy.

You can assign multiple categories to each service and task. This allows you to check the services or tasks that are associated with a specific work task or are the responsibility of a specific operator, as the situation requires.

You can assign categories when you add a service. Tasks inherit the categories of the service from which they are generated.

The following figure shows how you can display services and tasks by category.

Figure 1–23: Displaying services and tasks by category

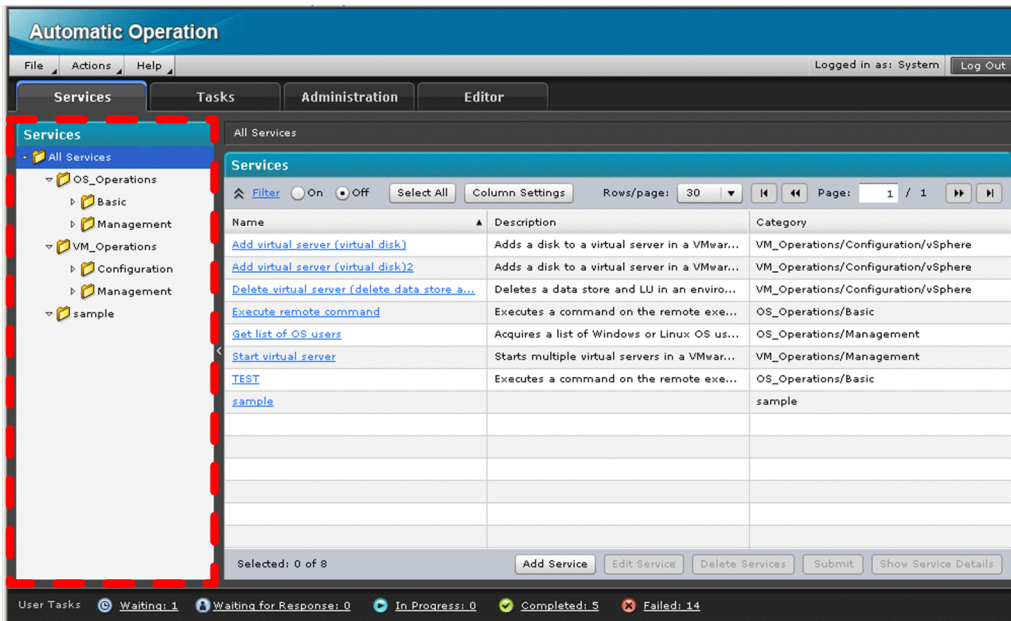


Services and tasks that belong to multiple categories appear under each of those categories in the JP1/AO user interface.

In the JP1/AO interface, the left pane shows the categories in a hierarchy (category tree), and the right pane shows the services and tasks that belong to the category selected in the left pane. The user interface only shows services and tasks that are associated with resource groups to which the user belongs.

The following figure shows an example of displaying services by category.

Figure 1–24: Displaying services by category



Any category that contains at least one service appears in the user interface. This means that the Tasks list might include categories that do not contain any tasks. Note that you cannot organize the History list by category. You can check the category of a task history under Category in the History list.

Related topics

- 4.1 Adding services

1.10 Managing users

You can register, edit, and otherwise manage the user accounts used to log in to JP1/AO. You can also lock user accounts. You need User Management permission to perform most user management operations. More than one user can have User Management permission.

You can also manage users by linking with the authentication function of JP1/Base.

User management in JP1/AO involves the following:

Registering users

Register the user accounts used to log in to JP1/AO.

Editing user information

A user with User Management permission can edit the profiles of all users. Users without User Management permission can edit their own profile.

Changing passwords

A user with User Management permission can change the passwords of all users. Users without User Management permission can change their own password.

You can set password criteria (such as minimum length and complexity) in the security definition file (`security.conf`).

Changing User Management permissions

You can control who can manage users in JP1/AO by assigning or revoking User Management permission.

If you change the permission of a logged-in user, the user keeps his or her original permissions while logged in. The system administrator must instruct any such users to immediately log out and log back in.

However, if the user opens a window (User Management, User Profile, Service Definition, Submit Service, Plan summary, Service Details, Task Details, or Respond) in a new browser window, the latest set of permissions for that user apply in the new browser window.

Locking and unlocking user accounts

You can lock and unlock user accounts.

If you lock the account of a logged-in user, that user will no longer be able to continue operations in JP1/AO.

A logged-in user cannot lock his or her own account. The account of a user who successively fails to log in a specified number of times is automatically locked. If all user accounts have been locked, you must use a command to unlock them.

You cannot lock and unlock the account of a user who logs in by using external authentication linkage.

Deleting user accounts

You can delete a user account registered with JP1/AO.

Important note

A user cannot manage or submit services without being assigned to a resource group and user group. Simply registering a user account is not sufficient.

Related topics

- [8.1 Registering users in JP1/AO](#)

- 8.2 Setting of another user's information by an administrator
- 8.3 Setting one's own user information
- 8.4 Changing of another user's password by an administrator
- 8.5 Changing one's own password
- 8.6 Changing the User Management permission settings
- 8.7 Locking users
- 8.8 Unlocking users
- 8.10 Deleting users from JP1/AO
- *Security definition file (security.conf) in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.10.1 Default user in JP1/AO

When you install JP1/AO, the following user account is registered by default:

System account

A user who can perform all operations and user management tasks in JP1/AO. You cannot delete this user or change the user's permissions.

The System account has access to all resources (services and connection destinations) in the JP1/AO system as an Admin role user.

When you first log in to a new installation of JP1/AO, log in as the System account user and create users with User Management permission as needed. The default password is *manager*. To prevent unauthorized access, we recommend that you change the password from the default.

Important note

The password of the System account is common across all Hitachi Command Suite products. If the password of the System account has already been changed in another Hitachi Command Suite product installed in your system, the default password will not apply.

Tip

User IDs are not case sensitive. Passwords are case sensitive.

1.10.2 Setting password criteria

You can set password criteria (such as minimum length and complexity) in a security definition file (`security.conf`).

Password criteria apply when you register a user or change a password. Because they do not apply to existing passwords, existing users will be able to log in to the JP1/AO system using passwords that do not meet the criteria.

For this reason, when password criteria are set, the system administrator should direct all users to immediately change their passwords.

In a cluster system, make sure to use the same setting on the primary and secondary node.

Related topics

- *Security definition file (security.conf) in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.11 Managing groups

JP1/AO uses resource groups and user groups to control the operation targets and functionality available to each user. A resource group is a group of resources (such as services and connection destinations), and a user group is a set of users who belong to the same organization or share similar responsibilities.

By allocating resource groups to user groups, you can control the access each user has to specific resources. By assigning a role to a resource group that defines which features of JP1/AO its members can use, you can set the functionality available to each user.

If you use the built-in resource group and built-in user group created at JP1/AO installation, you do not need to create groups before you start using JP1/AO.

The following describes what you can do with group management.

Create resource groups

You can create resource groups.

Edit resource groups

You can edit the name and description of resource groups as needed.

Delete resource groups

You can delete resource groups as needed.

You cannot delete a resource group that contains resources (services, tasks, histories, or connection destination definitions).

You can delete a resource group when a user group has a role associated with that resource group.

Create user groups

You can create a user group.

Edit user groups

You can add users to a resource group, change the resource groups allocated to a user group, and make other changes.

Allocate resource groups and roles to user groups

You can allocate resource groups to a user group. When you allocate a resource group to a user group, the users in that user group are able to manage and execute the services in that resource group.

You can also assign the Admin, Develop, Modify, or Submit role for each resource group you allocate.

If you change the user group permissions for a logged-in user, that user retains his or her original permissions during the login session. For this reason, the system administrator must instruct any such users to immediately log out and log back in.

Change the user group to which a user belongs

You can add and remove users to and from user groups.

Deleting user groups

You can delete user groups.

Deleting a user group does not delete the resource groups or users allocated to that user group.

Important note

If JP1/AO is installed on the same server as other Hitachi Command Suite products, the JP1/AO interface displays the resource groups and user groups for both JP1/AO and the Hitachi Command Suite products.

User groups in Hitachi Command Suite products

You can manage the user groups for Hitachi Command Suite products in JP1/AO. However, you cannot delete user groups that have been assigned roles in a Hitachi Command Suite product. To delete such a user group, first remove the role from the user group in the Hitachi Command Suite product. You cannot use the JP1/AO interface to change roles assigned in Hitachi Command Suite products.

Resource groups in Hitachi Command Suite products

You cannot manage resource groups for Hitachi Command Suite products in JP1/AO. Each product manages its own resource groups.

Related topics

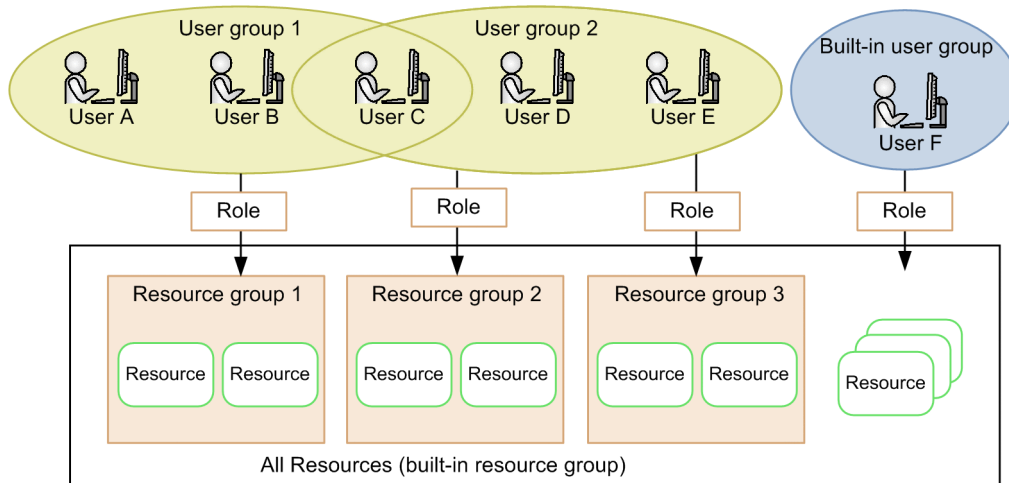
- [9.1 Creating resource groups](#)
- [9.2 Editing resource groups](#)
- [9.3 Deleting resource groups](#)
- [10.1 Creating user groups](#)
- [10.2 Editing user groups](#)
- [10.4 Assigning resource groups and roles to user groups](#)
- [10.5 Changing the user groups to which a user belongs](#)
- [10.6 Deleting user groups](#)

1.11.1 Access control using user groups and resource groups

A user group is a group which is created taking into consideration the type of organization or business and in which JP1/AO users are registered. A resource group is a group which is created at the level at which you want to control access and in which JP1/AO resources (such as services and connection destination definitions) are registered. To control access such as execution of services, or referencing tasks by using these groups, you must assign to each user group the resource groups to which you want to permit access.

The following figure shows an example of controlling accesses using user groups and resource groups.

Figure 1–25: Example of setting access control



In the example in the figure, users A, B, and C, who belong to user group 1, can use the resources in resource group 1. Users C, D, and E, who belong to user group 2, can use resources in resource groups 2 and 3. User F, who belongs to the built-in user group, has access to all services in JP1/AO because All Resources (built-in resource group) is assigned. Because of this, users A and B who belong to user group 1 only cannot reference services of resource groups 2 and 3.

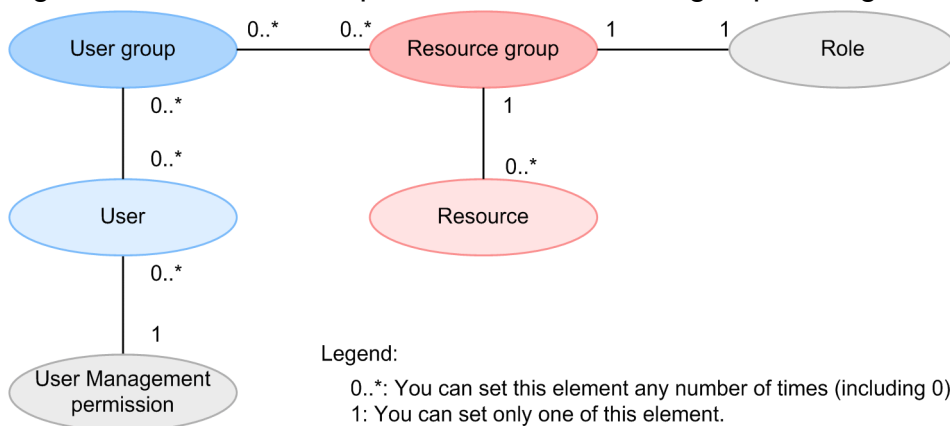
Group management in JP1/AO lets you efficiently control the access each user has to specific services in the context of user groups.

In scenarios such as a multi-tenant system of IT operation in a data center, you can sort the services used by each tenant into resource groups, thereby limiting the services each user group can execute. By doing so, you can avoid executing services of another tenant by mistake, and limit the range of tasks that can be referenced by each tenant.

1.11.2 Relationship between resource groups and user groups

The following figure shows how resource groups, user groups, and roles relate to each other.

Figure 1–26: Relationship between elements in group management



Resource groups

- Only users in the Admin role can manage resource groups.
- You can create multiple resource groups.
- Each resource group must have a different name.

- Every resource must belong to a resource group, but cannot belong to more than one. You can, however, allocate two separate resources with the same parameters to different resource groups.
- The built-in resource group All Resources is created automatically when you install JP1/AO.

User groups

- Only users with User Management permission can manage user groups.
- You can create multiple user groups.
- Each user group must have a different name.
- Users can belong to multiple user groups.
- You can assign several resource groups to one user group.
- AdminGroup, DevelopGroup, ModifyGroup, and SubmitGroup are created automatically as built-in user groups when you install JP1/AO.

Roles

- You can assign roles to resource groups. Only one role can be assigned to each resource group when assigning resource groups to user groups.

1.11.3 Built-in resource groups and built-in user groups

A built-in resource group and built-in user groups are created automatically when you install JP1/AO.

The built-in resource group All Resources contains all the services and connection destinations managed by JP1/AO.

JP1/AO provides the following built-in user groups:

AdminGroup

Assigns the Admin role for the All Resources resource group.

DevelopGroup

Assigns the Develop role for the All Resources resource group.

ModifyGroup

Assigns the Modify role for the All Resources resource group.

SubmitGroup

Assigns the Submit role for the All Resources resource group.

When you add users to these built-in groups, the users gain the permission associated with the assigned role for all resources in the JP1/AO system, allowing you to get up and running immediately.

Important note

- You cannot create, delete, rename, or change the description of a built-in resource group or built-in user group.
- JP1/AO also creates built-in user groups for the roles used with Hitachi Command Suite products. However, with JP1/AO, you can use only the AdminGroup, DevelopGroup, ModifyGroup, and SubmitGroup built-in user groups.

- If you install JP1/AO on a server where a Hitachi Command Suite product is installed, and a user group with the same name as the built-in user group already exists, the installer will not create a new instance of the built-in user group.

1.11.4 Types of roles that can be set for resource groups

In JP1/AO, you can control the functionality to which each user has access by assigning roles to resource groups.

Roles that can be set for a resource group varies depending on the resource group type. The following table shows the roles available by resource group.

Table 1–17: Roles available by resource group

Role	Available functionality	Can role be assigned?	
		All Resources	User-created resource group
Admin	<ul style="list-style-type: none"> • Resource group management • Service template management • Service template development • Service management • Service execution 	Y	N
Develop	<ul style="list-style-type: none"> • Service template management • Service template development • Service management • Service execution 	Y	N
Modify	<ul style="list-style-type: none"> • Service management • Service execution 	Y	Y
Submit	<ul style="list-style-type: none"> • Service execution 	Y	Y

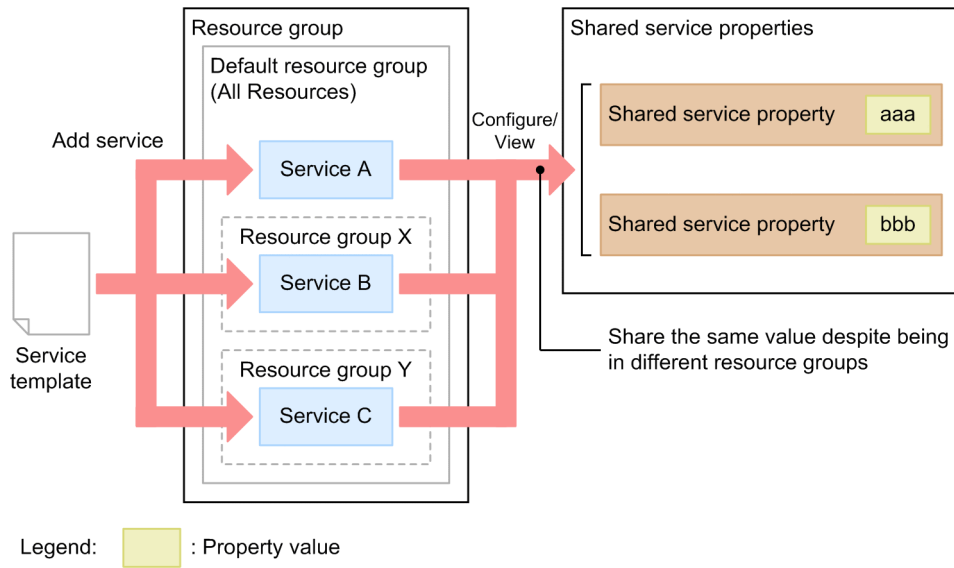
Legend:

Y: Can be assigned. N: Cannot be assigned.

1.11.5 Relationship between resource groups and shared service properties

The property value of a shared service property is shared across resource groups, even if services from a service template are added and allocated to different resource groups. You cannot assign a different value in each resource group because there is only one property value of the shared service property in a JP1/AO system.

Figure 1–27: Relationship between resource groups and shared service properties



1.12 Managing connection destination

In JP1/AO, the host to which a service connects to carry out operations is called a connection destination. By defining connection destinations in JP1/AO, when you submit services for execution, you can restrict access to connection destinations based on the resource group to which the tasks belong.

Important note

Immediately after installation, JP1/AO provides connection destination definitions that allow resource groups to connect to all connection destination hosts from All Resources services. This means that there are no restrictions on the connection destination hosts to which All Resources services can connect.

To impose restrictions on the hosts to which tasks can connect, you need to edit or delete the connection destination definition created at installation, and register connection destination definitions that limit connections to specific hosts.

To use the features for managing connection destinations, register the connection destinations to which you want to allow access in the **Connection Destinations** view. You can then edit registered connection destinations as needed.

Connection destination definition management lets you:

Create connection destination definitions

You can define and register connection destinations.

The definition of a connection destination consists of connection information such as a host name or IP address, and authentication information such as the user ID and password used to log in to the remote host.

Edit connection destination definitions

You can edit the definitions of connection destinations registered in the JP1/AO system.

Delete connection destination definitions

You can delete connection destinations registered in the JP1/AO system.

Related topics

- [11.1 Defining connection destinations](#)
- [11.2 Editing the definition information for connection destinations](#)
- [11.3 Deleting connection destinations](#)
- *Prerequisites for connection destinations in the Job Management Partner 1/Automatic Operation Overview and System Design Guide*

1.12.1 Access control using connection destination management

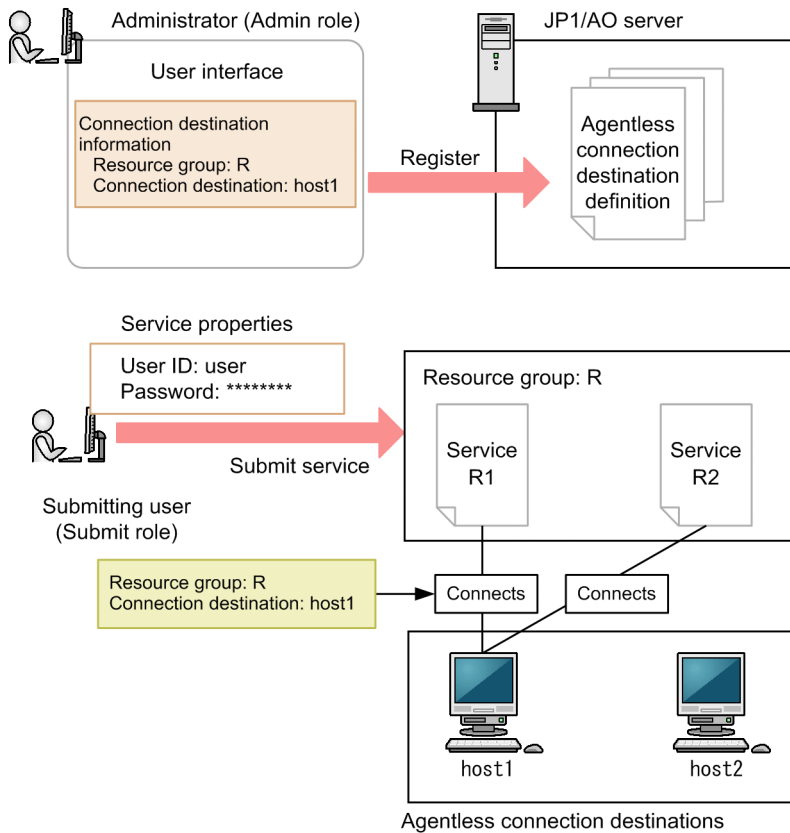
The feature for managing connection destinations consists of two sub-features: connection restriction and authentication information management. This section describes how access to connection destinations is controlled using the connection-restriction and authentication-information management features.

Connection-restriction

In JP1/AO, you can restrict access to connection destination hosts. This is called connection restriction.

You can permit access to a host by registering the host in advance as a connection destination in the JP1/AO system. The definition of a connection destination consists of the host name or IP address of the host, the destination type, the resource group, and other information. You can register connection destinations in the **Connection Destinations** view.

Figure 1–28: Accessing connection destinations (using connection restriction)

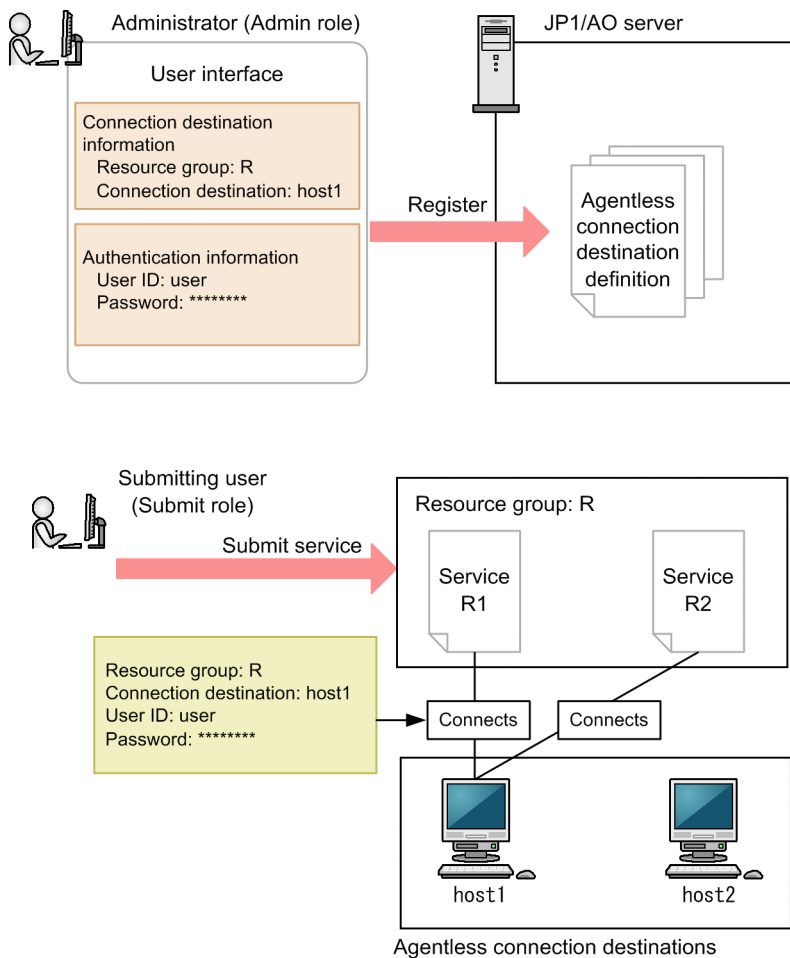


In this example, first, an administrator assigned the Admin role registers connection destination information from the JP1/AO interface. Then, a user assigned the Submit role submits various services to resource group R for execution, specifying his or her user ID and password. Here, the submitting user is permitted to connect to host1 only, and connections to other hosts are declined.

Authentication-information management

In addition to information about the connection destination, you can register authentication information such as the user ID and password needed to access the host. This is called authentication-information management. By registering this authentication information, you can use JP1/AO to manage passwords and other information that is used by a number of services. This lets you avoid repeatedly entering the same authentication information each time you submit a service for execution.

Figure 1–29: Accessing connection destinations (using authentication information management)



In this example, first, a user assigned the Admin role registers connection destination information and authentication information using the JP1/AO interface. Then, a user assigned the Submit role submits various services to resource group R for execution. Here, the submitting user is permitted to connect only to host1, on which connection destination information is registered, and connections to other hosts are declined. Also, because authentication information of host1 is registered in JP1/AO, it is not necessary to enter a user ID and a password to execute a service.

When you create a service template, you need to have registered the connection information and authentication information (if using authentication information management) used by the service template by the time the service is submitted for execution. The service will fail to connect to the connection destination if this information is missing. For this reason, information about connection destination hosts must be shared between the creator of the service template and the JP1/AO administrator.

Tip

JP1/AO can keep a record of definitions for a particular connection destination that result in successful connections. By using a definition that is proven to be successful, you can avoid failed authentication requests and other issues in situations where several sets of authentication information are defined for a single connection destination host.

JP1/AO updates the successful definitions accordingly when you edit connection destinations.

You cannot use successful agentless destination definitions immediately after you install JP1/AO, or if the maximum number of successful agentless destination definitions has been reached. In these situations, JP1/AO uses the authentication information registered in the connection destinations in no particular order.

Related topics

- [1.10 Managing users](#)
- [1.11.4 Types of roles that can be set for resource groups](#)

1.12.2 Configuring JP1/AO to reference authentication information of connection destination definitions

You can configure JP1/AO to reference authentication information specified in connection destination definitions when it executes a service.

The procedure and the timing for the configuration vary depending on the type of plug-ins you are using.

Basic plug-ins

For the following basic plug-ins, specify destination in the `credentialType` property when you create or edit a step. If you specify property in the `credentialType` property, the authentication information setting for connection destination definitions is not referenced because the property value of the plug-in is referenced. For details about how to set properties, see the related topics section for each plug-in in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

- General command plug-in
- File-forwarding plug-in
- Terminal connect plug-in

Content plug-ins

When you use the **Create Plug-in** dialog box to create a content plug-in, or use the **Edit Plug-in** dialog box to edit a content plug-in, select **Destination** in the **Credentials Type** area. If you select **Property** in this area, the property value of the plug-in is referenced rather than the authentication information setting for connection destination definitions.

1.12.3 List of definition parameters for connection destinations

Connection destination definitions consist of the following two types of information:

- Connection destination information
Permits connection to the connection destination. You must specify this setting if you intend to submit a service belonging to a resource group other than *All Resources* to connect to the connection destination.
- Authentication information
This information is used for authentication of connection destinations. You do not need to specify this setting if you do not specify authentication information as connection destination definitions.

The following table shows the parameters you can set when creating a definition for a connection destination.

Table 1–18: List of connection destination definition settings

Category	Item	Description
Connection destination information	Resource Group for Service	Specify the resource group name to associate with the connection destination. Services in this resource group only have access to connection destinations specified in the Destination field. If you specify All Resources, all services in All Resources will have access to all connection destinations.
	Type	Select one of the following: <ul style="list-style-type: none"> • Host Name^{#1} • IPv4 • IPv6
	Destination	Specify connection destinations in a format that matches the destination type. You can specify connection destinations in three ways: <ul style="list-style-type: none"> • Single destination • Range of destinations • All destinations
Authentication information ^{#2}	Protocol	Select one of the following authentication protocols to use when communicating with the connection destination host: <ul style="list-style-type: none"> • SSH • WMI • Telnet
	SSH authentication method	Specify the authentication method to use when communicating with the connection destination host. Specify one of the following methods if you select SSH as the protocol: <ul style="list-style-type: none"> • Password authentication • Public key authentication
	User ID	Specify the user ID of a user capable of remote login to the connection destination host. Specify domain user accounts in one of the following formats: <ul style="list-style-type: none"> • <i>domain-name\user-name</i> • <i>user-name@domain-name</i>
	Password	Specify the password corresponding to the user ID. You must specify the password if one of the following conditions applies: <ul style="list-style-type: none"> • When WMI is selected for the protocol • When Password authentication is selected for the SSH authentication method
	Superuser password ^{#3}	Specify the password for the superuser account at the connection destination host when you select SSH or Telnet for the protocol. Specification of the password for the superuser account varies depending on the definitions for the service template (whether to execute the command line or file transfer processing as a user with root privileges). Check the specifications of the service template and plug-ins to use.

#1

If the host name resolves to more than one IP address, JP1/AO allocates uses all of the IP addresses as the connection destination.

1. Using JP1/AO

#2

Set only one authentication information item for each connection destination. If you specify more than one authentication information item for the same connection destination, the authentication might fail.

#3

- For the General command plug-in, file-forwarding plug-in, and content plug-in, if the device to use runs on UNIX, use SSH for connection. To use SSH for connection, log in as the user specified for the user ID of authentication information. After the login, if you are prompted to elevate to a root user, edit authentication information (superuser password). The method for specifying whether to elevate to a root user varies depending on plug-ins.
 - For the General command plug-in and file-forwarding plug-in
Specify either true (elevate to a root user) or false (do not elevate to a root user) for the `elevatePrivileges` plug-in property.
 - For the content plug-in
To elevate to a root user, open the **Create Plug-in** or **Edit Plug-in** dialog box, and then select the **Execute by using root privileges (for SSH connections)**, or **Enabled** check box. Do not select either check box if you do not want to elevate.
- For the terminal command plug-in, if you specify the reserved `terminal.suPassword` reserved property as the command value of the `commandLine` plug-in property, specify the superuser password.
- For the General command plug-in, file-forwarding plug-in, and content plug-in, if you want to use SSH as the protocol for the connection with the connection destination, conditions exist for the shell specified as the default of the connection destination. The condition varies depending on whether to elevate to a root user. Specify as follows:
 - When elevating to a root user
Set the default shell of the connection user and the root user to `sh`, `bash`, `ksh`, `csh`, or `tcsh`.
 - When you do not want to elevate to a root user
Set the default shell of the connection user to `sh`, `bash`, `ksh`, `csh`, or `tcsh`.

Related topics

- [11.1 Defining connection destinations](#)
- [1.12.4 Resolving host names to IP addresses](#)
- *General command plug-in, File-forwarding plug-in, and Terminal command plug-in* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*

1.12.4 Resolving host names to IP addresses

If you specify Host Name for Type in the definition of a connection destination, JP1/AO performs IP address resolution when the service is submitted for execution. Specify a host name capable of IP address resolution by the OS. Host names defined only for `jp1hosts` or `jp1hosts2` of JP1/Base cannot be used.

If you specify a host name for the type when you edit or create a service template, you must also specify the host name in the plug-in properties. However, if you specify an IP address for the type, you can specify either the IP address or the host name in the plug-in properties. JP1/AO automatically converts the host names specified in the plug-in properties to IP addresses and uses them at the appropriate connection destinations.

The following table describes the correspondence between the destination type specified in the definition of the connection destination, and how connection destinations can be specified in the plug-in properties.

Table 1–19: Correspondence between connection types and connection destination specification

Destination type specified in connection destination	Connection destination specification in the plug-in properties		
	Host Name [#]	IPv4	IPv6
Host name	Y	N	N
IPv4	Y	Y	N
IPv6	Y	N	Y

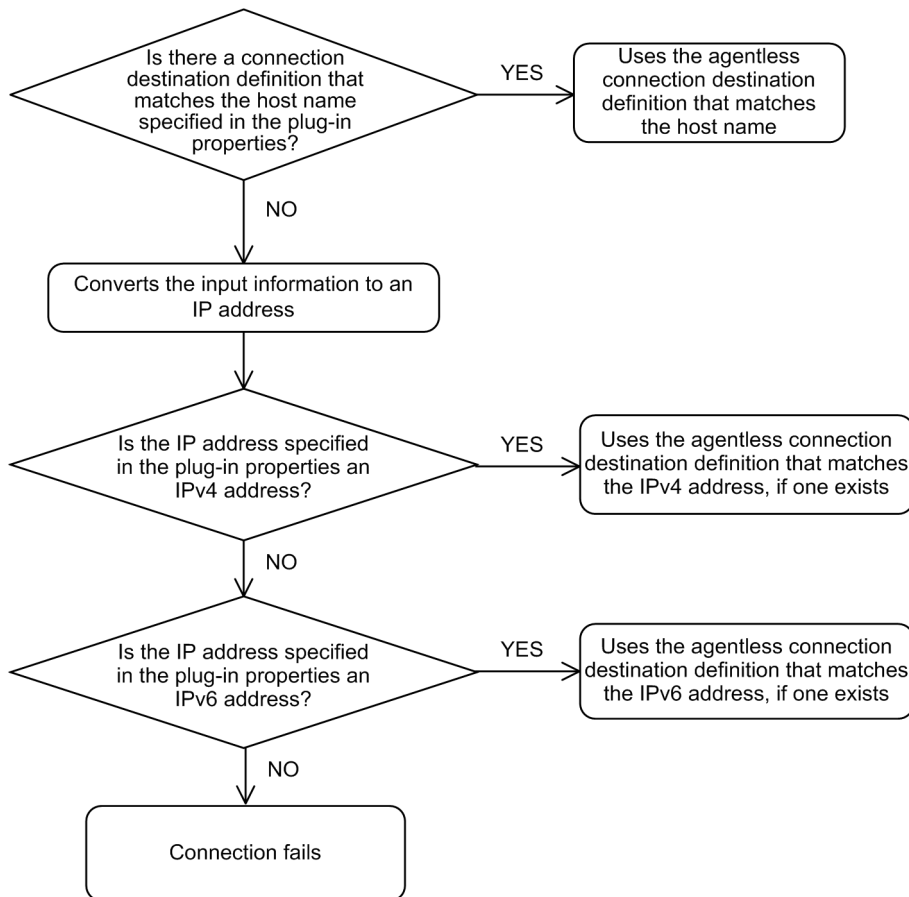
Legend:

Y: Can be specified. N: Cannot be specified.

#

When you specify a host name in the plug-in properties, JP1/AO uses the host name if it finds a definition of a connection destination that matches the host name. If there is no connection destination defined that matches the host name, JP1/AO converts the input information to an IP address. If the conversion process yields an IPv4 address, JP1/AO uses the IPv4 definition. If it yields an IPv6 address, JP1/AO uses the IPv6 definition. If there is no connection destination defined that matches the host name or IP address specified in the plug-in properties, the connection fails.

Figure 1–30: Behavior when host names are specified in the plug-in properties



1.12.5 Entry format for connection destinations

The format in which connection destinations are entered depends on the way in which the destination is specified (as a single destination, a range of destinations, or all destinations).

Table 1–20: Entry format for connection destinations

Type	How destination is specified	Entry format	Description
Host name	Single destination	Enter the connection destination in regular expression format. The pattern of the regular expression must conform to PCRE syntax. You can enter a regular expression that corresponds to several host names.	
	Range of destinations		
	All destinations	The comparison of the host names registered at a connection destination against the host names specified in the plug-in property is not case sensitive.	
IPv4	Single destination	<i>xxx . xxx . xxx . xxx</i>	Indicates the IP address <i>xxx . xxx . xxx . xxx</i> . <i>xxx</i> A number from 0 to 255. . A delimiter between numbers.
	Range of destinations	<i>xxx . xxx . xxx . aaa - bbb</i>	Indicates IP addresses in the range from <i>xxx . xxx . xxx . aaa</i> to <i>xxx . xxx . xxx . bbb</i> . <i>xxx</i> A number from 0 to 255. . A delimiter between numbers. <i>aaa</i> A number from 0 to 255. - A symbol indicating that a number range is specified. <i>bbb</i> A number from <i>aaa</i> +1 to 255.
	All destinations	*	Indicates all IP addresses. * A symbol that represents all IP addresses.
IPv6	Single destination	Specify a unicast address as defined in RFC2373.	
	Range of destinations	Specify an address range using a network prefix as defined in RFC2373.	
	All destinations	*	Indicates all IP addresses. * A symbol that represents all IP addresses.

Table 1–21: Examples of specifying connection destinations in IPv4 format

Example	Description
192 . 168 . 1 . 5	Indicates the IP address 192.168.1.5.
192 . 168 . 1 . 1 - 255	Indicates the IP addresses in the range from 192.168.1.1 to 192.168.1.255.
192 . 168 . 1 . 5 - 15	Indicates the IP addresses in the range from 192.168.1.5 to 192.168.1.15.
*	Indicates all IP addresses.

1.12.6 Default connection destinations

Immediately after installation, connection destination definitions that allow all resource groups to connect to all connection destination hosts from services in All Resources are already available.

Table 1–22: List of default parameters in connection destination definitions

Connection destination definition	Parameters	Value
For IPv4	Resource Group	ALL_RESOURCES
	Type	IPv4
	Destination	*
	Protocol	No default value
	SSH authentication method	No default value
	User ID	No default value
	Password	No default value
	Superuser password	No default value
For IPv6	Resource Group	ALL_RESOURCES
	Type	IPv6
	Destination	*
	Protocol	No default value
	SSH authentication method	No default value
	User ID	No default value
	Password	No default value
	Superuser password	No default value

1.13 Maintenance

This subsection describes how to perform maintenance in JP1/AO.

Backing up data in a JP1/AO system

You can back up the configuration information and database information of JP1/AO and JP1/Base.

Restoring data in a JP1/AO system

You can restore the JP1/AO and JP1/Base data that you backed up.

Database maintenance

You can use the `hcmdsdbtrans` command and the `ajsembdbbrorg` command to rebuild a database.

Starting the JP1/AO system

Use the `hcmds srv` command to start the JP1/AO system.

Stopping the JP1/AO system

Use the `hcmds srv` command to stop the JP1/AO system.

Related topics

- [12.1 Backing up data in a JP1/AO system \(non-cluster configuration\)](#)
- [12.2 Backing up data in a JP1/AO system \(cluster configuration\)](#)
- [12.3 Restoring data in a JP1/AO system \(non-cluster configuration\)](#)
- [12.4 Restoring data in a JP1/AO system \(cluster configuration\)](#)
- [12.5 Database maintenance \(non-cluster configuration\)](#)
- [12.6 Database maintenance \(cluster configuration\)](#)
- [12.7 Starting a JP1/AO system \(non-cluster configuration\)](#)
- [12.8 Starting a JP1/AO system \(cluster configuration\)](#)
- [12.9 Stopping a JP1/AO system \(non-cluster configuration\)](#)
- [12.10 Stopping a JP1/AO system \(cluster configuration\)](#)

1.13.1 Notes on backup and restoration

When you back up and restore data in a JP1/AO system, some of the detailed task information (step lists and progress information) is lost, and some task statuses are changed. Note that the progress and status of steps for restored tasks and debug tasks are not displayed in the **Task Monitor** view.

Depending on the status when a task and debug task are backed up, the status after restoration is changed. For details about statuses of tasks and debug tasks after restoration, see `restoresystem` (restoring the JP1/AO system) in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*.

Tasks and debug tasks in Waiting or Holding status when data was backed up enter Canceled status if they are restored. Note that you can re-register tasks in Waiting or Holding status (scheduled or recurring tasks) as another task with the same settings by using the `listtasks` and `submittask` commands.

To re-register a task, execute the `listtasks` command before the backup procedure, and output detailed task information. After restoration, use the `submittask` command to re-register detailed task information you output here in a batch. By doing so, you can re-register the task with the same settings as another task.

Note that you cannot redo tasks after restoration by selecting **Retry the Task From the Failed Step** or **Retry the Task From the Step After the Failed Step** in the **Tasks** view.

Related topics

- [1.6.11 Task categories and generation timing](#)
- [1.6.12 Task statuses and status transitions](#)
- [12.1 Backing up data in a JP1/AO system \(non-cluster configuration\)](#)
- [12.2 Backing up data in a JP1/AO system \(cluster configuration\)](#)
- [12.3 Restoring data in a JP1/AO system \(non-cluster configuration\)](#)
- [12.4 Restoring data in a JP1/AO system \(cluster configuration\)](#)

1.13.2 Notes on restarting JP1/AO services

When you restart a JP1/AO service, a task might fail depending on the task status when the service was stopped. The following table describes how tasks behave when a JP1/AO service restarts.

Table 1–23: Task behavior after a JP1/AO service restarts

No.	Task status when the JP1/AO service stops	Task behavior after the JP1/AO service restarts
1	Waiting	<ul style="list-style-type: none"> • If the system restarts before the scheduled start time: The task remains in the waiting status. • If the system restarts after the scheduled start time: The tasks starts executing immediately.
2	Holding	The task remains in the being held status.
3	Now running	The task fails.
4	Waiting for Response	The task fails.
5	Abnormal Detection	The task fails.
6	Terminated	The task fails.
7	Completed	The task remains in the ended normally status.
8	Failed	The task remains in the failed status.
9	Canceled	The task remains canceled.

1.13.3 Data that is restored

The following table lists the data that is restored.

Table 1–24: Data to be restored

No.	Type of data	Data that is restored
1	Execution information	Tasks
2	History information	Task histories
3	Definition information	Service templates

No.	Type of data	Data that is restored
4	Definition information	Services
5		Users, user groups, and resource groups
6		Definition of connection destinations
7		Service Share Properties
8	Definition files	Property files, email notification definition files, definition files used for JP1/IM linkage, and files under <i>JP1/AO-installation-destination-folder</i> \system\AJS3CD\conf
9	Task processing engine	Configuration information for the task processing engine

1.14 Linking with JP1/Base authentication

By linking with JP1/Base, you can use the authentication functionality of JP1/Base to manage and authenticate JP1/AO users.

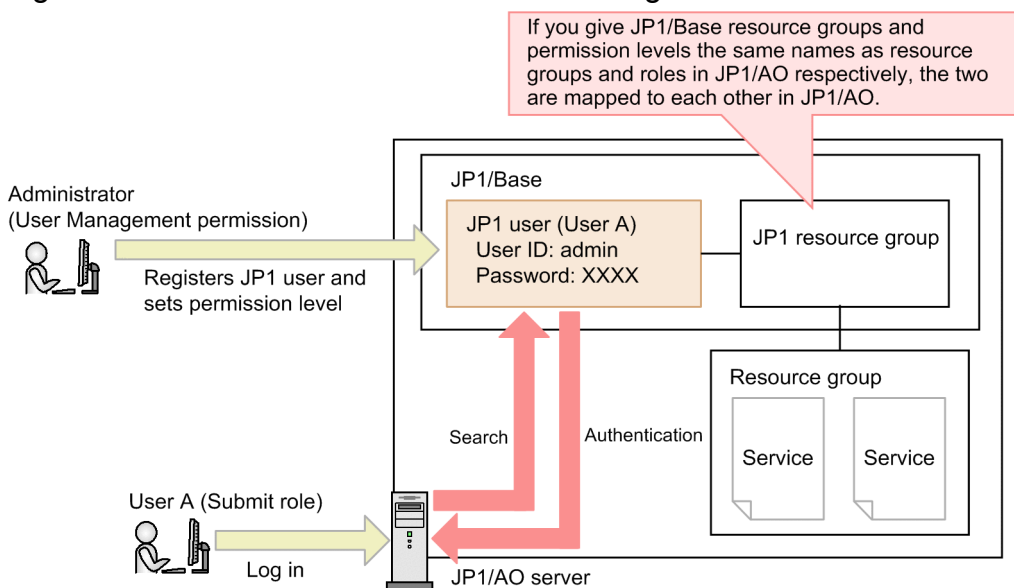
When you use JP1/Base to manage users, you can create users from the JP1/Base user interface and assign JP1 resource groups and permission levels. By giving JP1 resource groups and permission levels the same names as JP1/AO resource groups and roles respectively, you can manage JP1 users as JP1/AO users.

There are several advantages to linking with JP1/Base:

- You do not need to manage users and user groups in JP1/AO.
- You can use existing JP1 users.

The following figure shows a general overview of user authentication when linking with JP1/Base.

Figure 1–31: User authentication when linking with JP1/Base



To link JP1/AO with the authentication functionality of JP1/Base, you need to set a configuration file for external authentication server linkage. In a cluster system, make sure that you use the same settings on the primary and secondary nodes.

After linking with the JP1/Base authentication functionality, when you log in to JP1/AO from a user account that is not registered in JP1/AO, the authentication process is performed by JP1/Base. When a user registered in JP1/AO logs in to JP1/AO, authentication and permissions are managed by JP1/AO without any involvement by JP1/Base.

Related topics

- *Linking to the JP1/Base authentication function in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.15 Linking with Active Directory

By linking with Active Directory, you can use users and groups managed by Active Directory in JP1/AO. Note, however, that you can link with Active Directory when JP1/AO uses Active Directory as the LDAP directory server.

To enable Active Directory linkage, you must set the configuration file for external authentication server linkage. In addition, if necessary, register a user or a user for LDAP search in Active Directory.

Also, when using the Active Directory linkage function, you can select whether to enable group linkage. Depending on whether group linkage is used, available functions differ.

- When group linkage is not used
 - Active Directory authenticates users.
 - JP1/AO registers or deletes users in/from a user group.
 - For this purpose, the same users must be registered in JP1/AO and Active Directory. When doing so, you do not need to set passwords for JP1/AO.
- When group linkage is used
 - Active Directory authenticates users.
 - Register and use Active Directory groups as JP1/AO user groups. Active Directory registers or deletes a user in/from a group.
 - As a result, you do not register users in JP1/AO .

Next, advance registrations and the user authentication flow when group linkage is not used, or when group linkage is used separately.

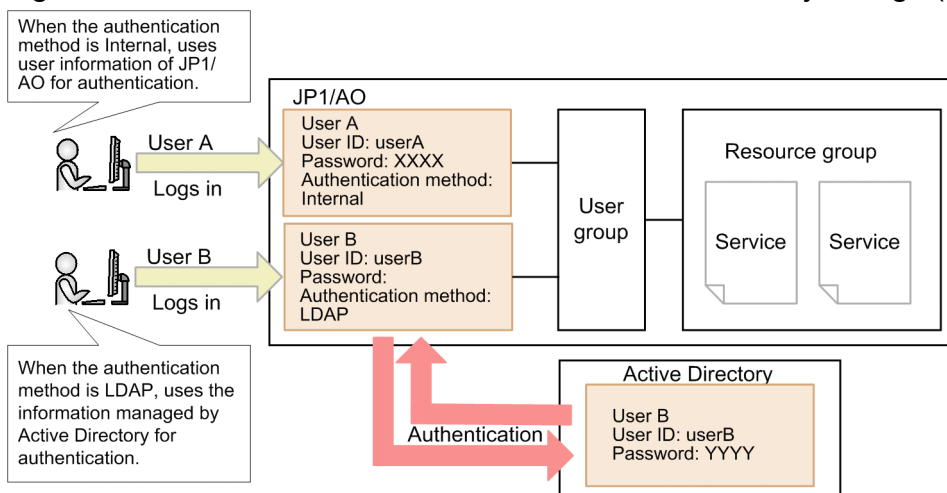
When group linkage is not used

Match a JP1/AO user ID and an Active Directory user ID as a user who logs in to JP1/AO for registration. It will be no longer necessary to manage passwords in JP1/AO just by registering them in Active Directory.

If LDAP is specified for the authentication method in JP1/AO user information when a user logs in to JP1/AO, you can use information managed by Active Directory for the login.

The following figure shows the user authentication flow when Active Directory linkage does not use group linkage.

Figure 1–32: User authentication flow for Active Directory linkage (when group linkage is not used)



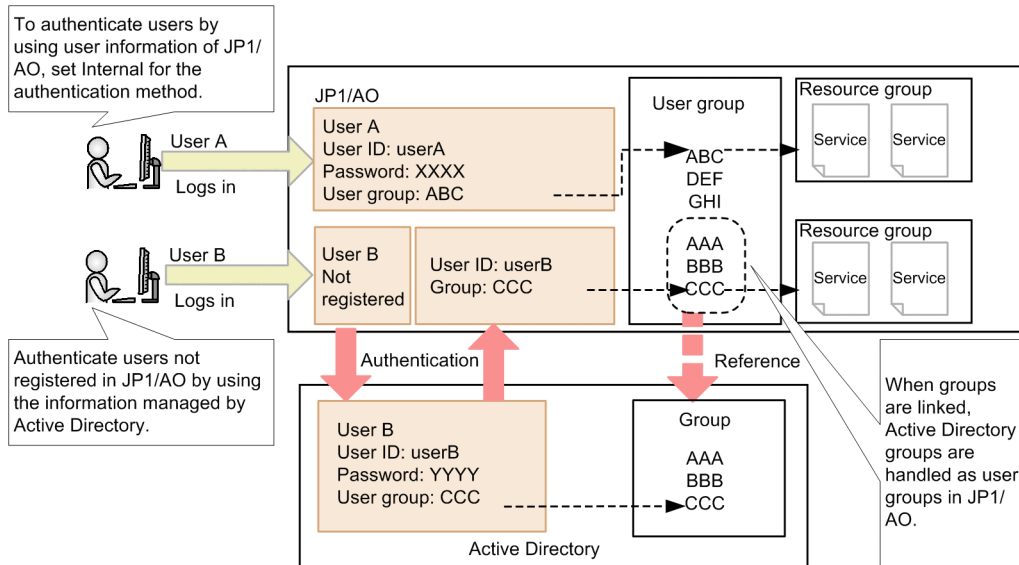
When group linkage is used

You can manage Active Directory groups as JP1/AO user groups. As a result, you do not need to register users registered in Active Directory groups in JP1/AO. By allocating a resource group to an Active Directory group, you can use the resource.

If user information is not registered in JP1/AO when a user logs in to JP1/AO, it references user information in Active Directory to allow the login.

The following figure shows the user authentication flow when Active Directory linkage uses group linkage.

Figure 1–33: User authentication flow for Active Directory linkage (when group linkage is used)



Related topics

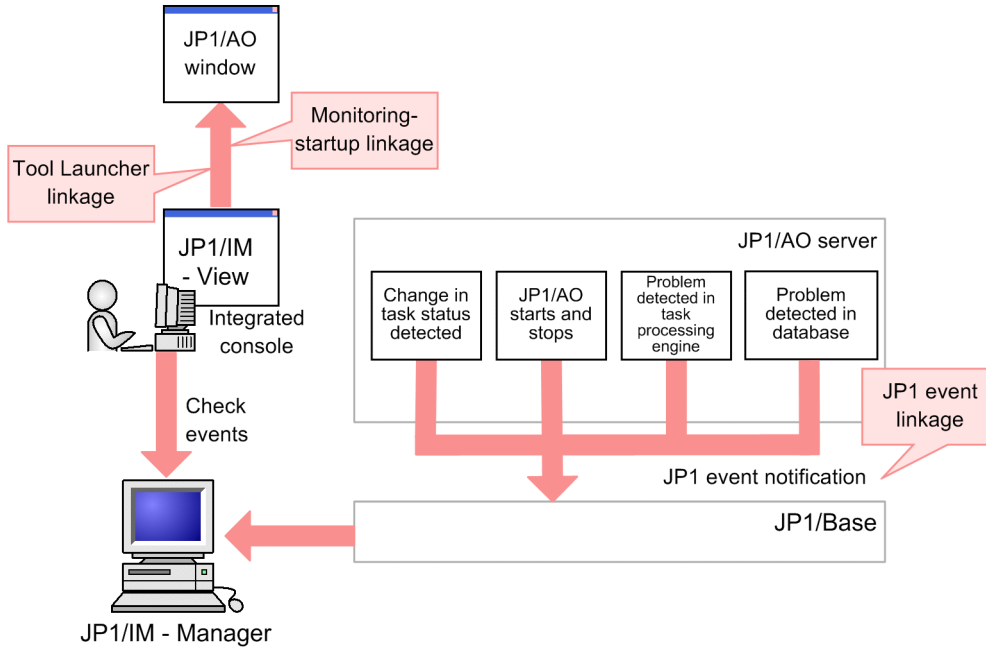
- *Linking with Active Directory in the Job Management Partner 1/Automatic Operation Configuration Guide*
- [8. Managing Users](#)
- [10. Managing User Groups](#)

1.16 Linking with JP1/IM event monitoring

JP1/IM is an product that links with products in the JP1 series and other middleware to manage the configuration and operation of entire systems from an integrated perspective.

By linking JP1/AO with JP1/IM, you can centrally monitor JP1 events issued by JP1/AO in JP1/IM.

Figure 1–34: Overview of JP1 event reporting



By linking with the event monitoring functionality of JP1/IM, you can:

Use JP1 event linkage

JP1 events are forwarded to JP1/IM - Manager via JP1/Base[#]. As a result, you can centrally monitor JP1 events from the **Event Console** window of JP1/IM - View.

JP1/AO issues a JP1 event when a change in task status is detected, when JP1/AO starts and stops, when a problem is detected in the task processing engine, and when a problem is detected in the database.

#

In a non-cluster configuration, JP1/AO reports JP1 events to the instance of JP1/Base on the same host. In a cluster environment, JP1 events are reported to the instance of JP1/Base on a host that has the same logical host name as the JP1/AO host.

Use monitoring-startup linkage

By defining the window to be called in JP1/IM -View, you can display a JP1/AO window associated with a JP1 event. For example, when investigating a JP1 event that reports a failed JP1/AO task, you can launch the JP1/AO window that shows the result of the task.

Use Tool Launcher linkage

By adding JP1/AO to the JP1/IM - View Tool Launcher, you can display the JP1/AO interface from JP1/IM - View.

Related topics

- [A.1\(1\) List of JP1 events](#)

- *Linking to the JP1/IM event monitoring function in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.16.1 Timing of JP1 event reporting

You can use JP1/IM to centrally monitor the JP1 events issued by JP1/AO. The following table describes the timing with which JP1/AO issues JP1 events.

Table 1–25: Timing of JP1 event notification

Timing		Event ID
Category	Subcategory	
Task status detected ^{#1}	A task enters Waiting for Response status ^{#2}	0x00007000
	A task enters Completed status	
	A task enters failed status	
	A task enters Canceled status	
JP1/AO operating status	JP1/AO starts	0x00007010
	JP1/AO shuts down	
Error detected in task processing engine	An error occurs when you execute a task processing engine command.	0x00007020
Error detected in database ^{#3}	An error occurs when attempting to connect to the database	0x00007030

#1

JP1/AO monitors the status of tasks at regular intervals (once every 30 seconds by default). The JP1 event is generated when JP1/AO detects the change, not when the change itself occurs. JP1/AO will not issue additional events until the status changes again.

#2

If a task transitions to the waiting for response status and the user enters a response in less than 30 seconds in the **Respond** dialog box, the JP1 event reporting the change to the waiting for response status might not be issued because the task has already transitioned to another status.

#3

JP1 events resulting from the same occurrence will not be issued for the next hour after the first notification.

Tip

If there are too many events generated by the task processing engine and it becomes difficult to identify events issued by JP1/AO, filter the events in the JP1/IM interface.

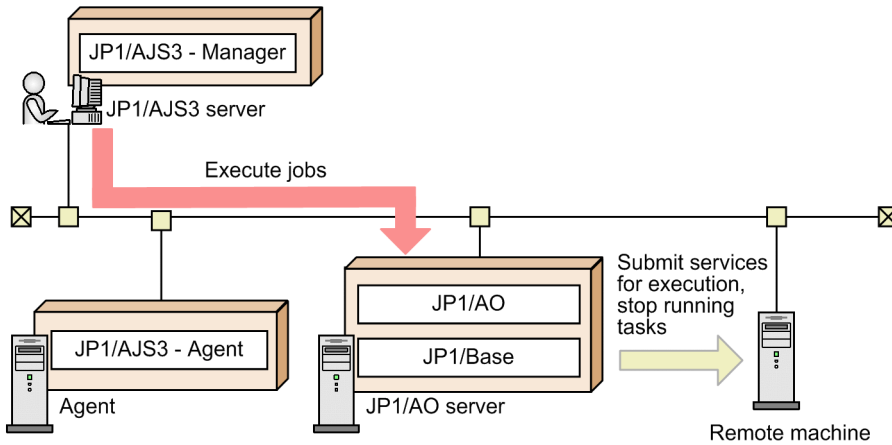
1.17 Linking with JP1/AJS3

By linking with JP1/AJS3, you can execute the following commands automatically for the JP1/AO server from the JP1/AJS3 server:

- `stoptask` command
- `submittask` command

The following figure provides an overview of linkage with JP1/AJS3.

Figure 1–35: Overview of JP1/AJS3 linkage



To link with the JP1/AJS3 server, register JP1/AO as the execution agent. In addition, create a PC job to be executed in the JP1/AO server.

Related topics

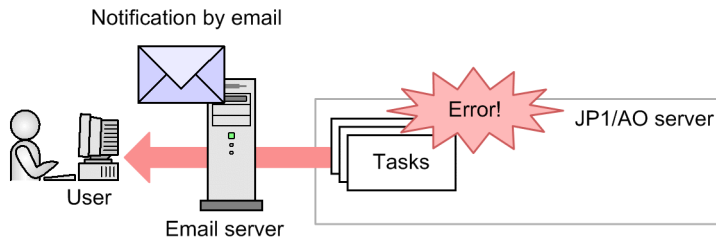
- *Linking with JP1/AJS3* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

1.18 Email notification

You can configure JP1/AO to send a notification email when it detects a task error or failure. To use this feature, you must enter the required information in a shared built-in service property and email notification definition file.

The following figure shows an overview of email notification:

Figure 1–36: Overview of email notification



The following describes the functionality provided by email notification:

Email notification

You can use the SMTP server built in to the JP1/AO system to send email in text format reporting the abnormal status of a task.

An email notification is sent when:

- JP1/AO detects that a task has entered an abnormal status
- JP1/AO detects that a task has entered Failed status

Note that JP1/AO does not send an email notification if a task fails because it was stopped by a user. Email notifications are also not sent if the task was in Abnormal Detection or Terminated status before transitioning to Failed status.

Email notification is also performed if you execute a service generated from a service template that uses the Email notification plug-in.

Related topics

- [1.7.2 List of shared built-in service properties](#)
- *Definition file for email notification (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, and `mailDefinition_zh.conf`) in the *Job Management Partner 1/Automatic Operation Configuration Guide*.*
- *Email Notification Plug-in in the manual *Job Management Partner 1/Automatic Operation Service Template Reference**

1.18.1 List of email notification settings

To send email notifications, set the shared built-in service properties, the properties file (`config_user.properties`), and the email notification definition files (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, and `mailDefinition_zh.conf`).

The following table lists the settings that relate to email notification.

Table 1–26: List of email notification settings

Item	Where to set	Whether required
Whether email notification available	Shared built-in service properties	Required
SMTP server IP address or host name		Required
SMTP server port number		Required
SMTP server user ID		Required
SMTP server password		Required
Notification email sender ^{#1}		Required
Notification email recipients (TO)		Required
Notification email recipients (CC)		Arbitrary
Notification email recipients (BCC)		Arbitrary
Number of retry attempts and retry interval when email notification cannot be sent	Properties file (<code>config_user.properties</code>)	Arbitrary ^{#2}
Email notification subject and message text	Email notification definition files (<code>mailDefinition_ja.conf</code> , <code>mailDefinition_en.conf</code> , and <code>mailDefinition_zh.conf</code>)	Arbitrary ^{#2}

#1

Also used as the email notification reply-to address.

#2

Change the default value set in the properties file (`config_user.properties`) or the email notification definition file (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, and `mailDefinition_zh.conf`) if necessary.

The encoding for notification emails is UTF-8. The configuration of the SMTP server (such as restrictions on character counts) can affect the contents of notification emails. Check the configuration of the SMTP server before you set the parameters for notification emails.

Related topics

- [1.7.2 List of shared built-in service properties](#)
- *Properties file (`config_user.properties`) and email notification definition files (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, and `mailDefinition_zh.conf`) in the JPI/AO Job Management Partner 1/Automatic Operation Configuration Guide*

1.19 Direct-access URLs

You can display a specific part of the JP1/AO interface immediately after you log in by specifying the URL of the window in a direct-access URL.

When you log in with a direct-access URL specified, JP1/AO does not display the intervening windows that usually appear between the **Login** window and the target window.

You can specify the following dialog boxes as a direct-access URL:

- **Service Definition** dialog box
Window in which you can check and change service information
- **Submit Service** dialog box
Window in which you can submit services for execution
- **Task Details** dialog box
Window in which you can view detailed information about tasks

1.19.1 Format and parameters of direct-access URLs

A direct-access URL consists of a launch URL that specifies the window to display, and query parameters which specify the information to be displayed in that window. The launch URL and query parameters are delimited by a question mark (?).

The character that can be specified as the first character of the direct-access URL varies depending on the method of communication between Web browser and JP1/AO server. The following figure provides an example for HTTP connection, but replace it with HTTPS if necessary.

Figure 1–37: Specification format of a direct access URL (for the **Task Details** dialog box)

```
http://host-name:port-number/Automation/launcher/TaskDetails?task_id=task-ID
```

If you specify a launch URL incorrectly, an error message delivered by the Web client or Web server appears instead of the **Login** window.

If you specify a query parameter incorrectly, an error message is displayed in the **Login** window.

The following are the specification formats of the direct access URLs for opening dialog boxes.

- For the **Service Definition** dialog box
`http://host-name:port-number/Automation/launcher/ConfigService?rg=resource-group-name-of-service&sn=service-name`
- For the **Submit Service** dialog box
`http://host-name:port-number/Automation/launcher/SubmitTask?rg=resource-group-name-of-service&sn=service-name&tn=task-name&td=task-description&pr_property-key=property-value#`

Multiple `pr_property-key=property-value` specifications are allowed if you use `&` between specifications, such as `&pr_property-key1=property-value1&pr_property-key2=property-value2....`

- For the **Task Details** dialog box

`http://host-name:port-number/Automation/launcher/TaskDetails?task_id=task-ID`

Parameters of a direct-access URL

The following table shows the parameters of a direct-access URL.

Table 1–27: Parameters of a direct-access URL

No.	Component	Parameter	Description
1	Launch URL	<i>host-name</i>	Specifies the host name or IP address of the JP1/AO server.
2		<i>port-number</i>	Specifies the port number of the JP1/AO Web server.
3	Query parameters	<i>rg=resource-group-name-of-service</i>	Specify the name of the resource group that contains the service you want to display, as a URL-encoded ^{#1} character string. You can find the resource group for a service by looking in the JP1/AO windows. You can also find it in the Resource Group column in the file output by the <code>listservices</code> command.
4		<i>sn=service-name</i>	Specify the name of the service you want to display as a URL-encoded ^{#1} character string (the character set is UTF-8). You can find the service name by looking in the JP1/AO windows. You can also find it in the Service Name column in the file output by the <code>listservices</code> command, which outputs a list of services.
5		<i>task_id=task-ID</i>	Specify the ID of the task you want to display. You can find the task ID by looking in the JP1/AO windows. You can also find it in the TaskID column in the file output by the <code>listtasks</code> command, which outputs a list of tasks.
6		<i>tn=task-name^{#2}</i>	Specify the name of the task you want to enter as a URL-encoded ^{#1} character string (the character set is UTF-8). You can specify a maximum of 128 characters for the value.
7		<i>td=task-description^{#2}</i>	Specify a description of the task you want to enter as a URL-encoded ^{#1} character string (the character set is UTF-8). You can specify a maximum of 256 characters for the value.
8		<i>pr_property-key=property-value^{#2}</i>	Specify the property key and the property value you want to enter. To specify this parameter more than once, use <code>&</code> , such as <code>&pr_property-key1=property-value1&pr_property-key2=property-value2...</code> Specify the property value as a URL-encoded ^{#1} character string (the character set is UTF-8). The property value specified as a direct access URL is applied only to the Submit Service dialog box. It is not applied to the Service Definition dialog box and the shared service property settings.

#1

URL-encoded means processing that converts characters that cannot be read by a Web browser as a URL to characters that can be read.

For example, the following is a URL used to display the **Service Definition** dialog box:

Service settings

host-name: host01

port-number: 23015

resource-group-name: All Resources

service-name: JP1/AJS jobnet execution registration

URL to specify

```
http://host01:23015/Automation/launcher/ConfigService?rg=All
%20Resources&sn=JP1%2fAJS%e3%82%b8%e3%83%a7%e3%83%96%e3%83%8d
%e3%83%83%e3%83%88%e5%ae%9f%e8%a1%8c%e7%99%bb%e9%8c%b2
```

#2

The number of characters that can be specified as a query parameter is limited. For details about the formula for estimating and checking the number of characters in a query parameter, see [1.19.2 How to estimate the number of characters in a query parameter](#).

The following table explains whether items to specify for a dialog box to be displayed can be omitted.

Table 1–28: Items that can be omitted

No.	Component	Parameter	Service Definition dialog box	Submit Service dialog box	Task Details dialog box
1	Launch URL	<i>host-name</i>	N	N	N
2		<i>port-number</i>	N	N	N
3	Query parameters	<i>rg=resource-group-name-of-service</i>	N	N	--
4		<i>sn=service-name</i>	N	N	--
5		<i>task_id=task-ID</i>	--	--	N
6		<i>tn=task-name</i>	--	Y	--
7		<i>td=task-description</i>	--	Y	--
8		<i>pr_property-key=property-value</i>	--	Y	--

Legend:

Y: Can be omitted, N: Cannot be omitted, --: Cannot be specified.

Notes on specifying query parameters

- Use ASCII characters for a query parameter.
- The maximum number of characters that can be specified is 1,024.
- A character string that contains URL-encoded surrogate pair characters or control characters cannot be specified.
- The following are characters that can be specified for a query parameter:
 - Half-width letters (a to z and A to Z)
 - Half-width numbers (0 to 9)
 - Half-width hyphen (-)
 - Half-width underscore (_)
 - Half-width period (.)
- If you specify a query parameter that uses specifiable characters, but is not listed in the Parameter column in the table, the query parameter is ignored.
- If you did not specify a value for a query parameter that can be omitted, no value is set.
- Carefully consider security when you specify passwords or other confidential information in a direct access URL.

How to specify `pr_property-key=property-value`

- Specify an input property displayed in the **Submit Service** dialog box as a property key.
- You must specify a property value for a property that must be specified and whose data type is either *list* or *boolean*.
- The format for specifying a query parameter is determined by the data type of the property. The following table describes specification formats for each data type.

Table 1–29: Specification formats for each property data type

Parameter data type	Format
string	Specify a character string of no more than 1,024 characters.
boolean	Specify <code>true</code> or <code>false</code> .
integer	Specify an integer from -2,147,483,648 to 2,147,483,647.
double	Specify a double floating-point number from approximately $\pm 4.9 \times 10^{-324}$ to $\pm 1.7 \times 10^{308}$.
date	Specify the date in <i>YYYY-MM-DD</i> format. You can specify a date from 1900-01-01 to 2100-12-31. <ul style="list-style-type: none">• <i>YYYY</i>: Year• <i>MM</i>: Month• <i>DD</i>: Day
password	Specify a character string of no more than 1,024 characters.
list	Specify a property value that is displayed in the list box.

1.19.2 How to estimate the number of characters in a query parameter

You can specify a maximum of 1,024 characters for the query parameter of a direct access URL. Use the following formula to verify the number of characters that are specified for a query parameter:

$(\text{number-of-characters-for-resource-group-name} + \text{number-of-characters-for-service-name} + \text{number-of-characters-for-task-name} + \text{number-of-characters-for-task-description}) + 16 + (\text{number-of-characters-for-property-key} + \text{number-of-characters-for-property-value} + 5) \times n^{\#} \leq 1,024$

#: *n* is the number of properties to be specified.

1.20 Configuring Link&Launch

If you set Link&Launch, the **Tools** menu appears in the menu area, from which you can launch Hitachi Command Suite products in single sign-on mode.

Hitachi Command Suite products to start must be installed on the JP1/AO server. In addition, the host name must be resolved correctly because the host name or the IP address specified during installation of each Hitachi Command Suite product is used.

Set Link&Launch in the properties file (`config_user.properties`).

The table below lists products for the Link&Launch function, and the order displayed on the **Tools** menu. Note that names of Hitachi Command Suite products that are not installed on the JP1/AO server are deactivated.

Table 1–30: Products compatible with Link&Launch

No.	Product	Display order
1	Hitachi Device Manager Software	1
2	Hitachi Tuning Manager Software	2
3	Hitachi Global Link Manager Software	3
4	Hitachi Replication Manager Software	4
5	Hitachi Compute Systems Manager Software	5

Before you can use Link&Launch, you need to define the property file and set permission levels in JP1/Base.

Related topics

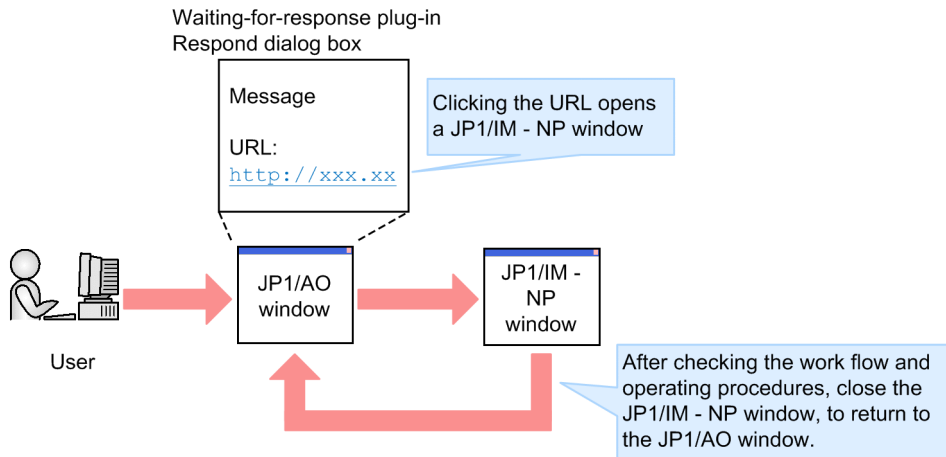
- *Properties file (config_user.properties) and Defining permissions in JP1/Base (for single sign-on to all Hitachi Command Suite products) in the Job Management Partner 1/Automatic Operation Configuration Guide*

1.21 Linking with JP1/IM - NP business content

From a JP1/AO window, you can launch a JP1/IM - NP window in single sign-on mode. The **Respond** dialog box showing the JP1/IM - NP business content (workflow and guide) for checking workflow and operating procedures.

The following figure provides a general overview of linking with JP1/IM - NP business content.

Figure 1–38: Overview of linking with JP1/IM - NP business content



To link with JP1/IM - NP, JP1/AO and JP1/IM - NP must use the same JP1/Base authentication functionality.

Related topics

- *User-response Wait Plug-in* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*

2

Logging in to JP1/AO

This chapter describes how to log in to JP1/AO.

2.1 Logging in to JP1/AO

Log in to JP1/AO by entering the login URL in a Web browser.

Who can perform this task:

All users

To log in to JP1/AO:

1. Use your Web browser to access the login URL.

2. Enter your user ID and password.

The first time you log in to a new installation of JP1/AO, log in as the following user and create users with User Management permission as needed.

- User ID: system
- Password: manager

To prevent unauthorized access, we recommend that you change the password of the System account.

3. Click the **OK** button.

Login URL:

The URL used to log in to JP1/AO depends on whether JP1/AO is operating in a cluster environment.

Table 2–1: Login URL:

System configuration	URL	How to specify
Non-cluster system	For HTTP connection <code>http://host-name-or-IP-address:port-number/ Automation/</code> For HTTPS connection <code>https://host-name-or-IP-address^{#1}:port-number/ Automation/</code>	<ul style="list-style-type: none">• As <i>host-name-or-IP-address</i>, specify the host name or IP address you specified when installing JP1/AO.• The default for <i>port-number</i> is 23015 for HTTP connection, and 23016 for HTTPS connection. Note that you can change the port number from the default.
Cluster system	For HTTP connection <code>http://logical-host-name-or-logical-IP-address:port- number/Automation/</code> For HTTPS connection <code>https://logical-host-name-or-logical-IP-address^{#1}:port- number/Automation/</code>	The default for <i>port-number</i> is 23015 for HTTP connection, and 23016 for HTTPS connection. Note that you can change the port number from the default. ^{#2}

#1

For HTTPS connection, we recommend that you specify the host name if the host name is specified for SSL server certificate, or the IP address if the IP address is specified as the URL. If they do not match, a warning or error message is displayed.

#2

When changing the port number of JP1/AO in a cluster system, stop the service in the cluster software. When changing the port number, you must do so on the primary and secondary host.

Related topics

- [1.10.1 Default user in JP1/AO](#)

- [12.10 Stopping a JP1/AO system \(cluster configuration\)](#)
- Procedure to change the port number in the *Job Management Partner 1/Automatic Operation Configuration Guide*

3

Managing service templates

This chapter describes how to manage service templates in JP1/AO.

3.1 Developing service templates

You can develop service templates that are required to automate operating procedures.

Who can perform this task:

Users in the Admin role or the Develop role who also have Administrator permissions for the OS

To develop a service template:

For details about how to develop service templates, see the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

3.2 Adding (importing) a service template to JP1/AO

The following describes how to add service templates selected according to intended use to JP1/AO. Adding service templates to JP1/AO is called importing service templates.

Who can perform this task:

Users in the Admin role or the Develop role who also have Administrator permissions for the OS

To add a service template to JP1/AO:

From the command prompt, execute the `importservicetemplate` command.

The service template is imported into the JP1/AO server.

You can view the service templates you have added in the **Add Service** dialog box.

Tip

- If you built or released a service template, it is imported automatically without executing the `importservicetemplate` command.
- If you want to import several service template files (st files) at once, you can do so in one operation by creating a zip file that contains the st files you want to import. Do not use folders in the zip file.

Related topics

- [1.3.2 Storage location of service templates in JP1/AO standard-package plug-ins and JP1/AO Content Set](#)

3.3 Deleting service templates from JP1/AO

You can delete service templates that are no longer required from JP1/AO.

Criteria for deleting service templates:

Before you can delete a service template, you must delete all of the services that were generated from that service template.

Important note

When you delete a service template, the service template configuration file under the service template storage folder, and the shared service properties that were used by the service template are also deleted. However, they are not deleted if shared service properties are being used in other service templates.

Who can perform this task:

Users in the Admin role or the Develop role who also have Administrator permissions for the OS

To delete service templates from JP1/AO:

To delete the release service template, execute the `deleteservicetemplate` command from the command prompt.

The selected service templates are deleted from the JP1/AO server.

You can make sure that the service templates were deleted by confirming that they no longer appear in the **Add Service** dialog box.

Tip

Delete the development service template in the **Editor** window.

Related topics

- [4.3 Deleting services](#)
- Procedure for deleting development service templates in the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*

3.4 Adding preset properties to service templates

You can add preset properties to a service template.

Who can perform this task:

Users who have Administrators permission for the OS

To add preset properties to a service template:

1. Prepare a preset property definition file.

Name the preset property definition file in `preset_preset-name.properties` format. Specify 1 to 30 characters for *preset-name*.

The following are the characters you can specify for *preset-name*:

- Half-width alphanumeric characters
- Half-width hyphen (-)
- Half-width underscore (_)
- Half-width period (.)

2. Save the preset property definition file in the following folder.

In a non-cluster system:

```
JPI/AO -installation-folder\extra_presets\vendor-ID-of-service-template\service-template-ID  
\service-template-version
```

In a cluster system:

```
shared-folder-name\jplao\extra_presets\vendor-ID-of-service-template\service-template-ID  
\service-template-version
```

The preset properties are added to the service template.

You can view the added preset properties in the **Service Definition** dialog box of the service that was added from the applicable service template. In the **Service Definition** dialog box, select *preset-name* to apply the change, which sets the values for the properties all at once.

Related topics

- [1.8.1 About preset property definition files](#)
- [1.8.2 Preset property definition file format](#)
- *Property file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

3.5 Outputting (exporting) service template lists

Use the procedure described here to output a list of service templates to a CSV file. Outputting a list of service templates is also called exporting a list of service templates.

You can use the list to find out which service templates are available in JP1/AO.

Who can perform this task:

Users in the Admin role, Develop role, or Modify role who also have Administrator permissions for the OS

To output a list of service templates:

From the command prompt, execute the `listservices` command with `servicetemplates` specified in the `/output` option.

A list of service templates is output as a CSV file to the location specified in the command.

4

Managing services

This chapter describes how to manage services in JP1/AO.

4.1 Adding services

This section describes how to add service templates that have been added to JP1/AO to the list of services (**Services**) in the **Services** window. After adding a service to the **Services**, you can then submit the service for execution.

Tip

You can add more than one service from the same service template.

Who can perform this task:

Users in the Admin role, Develop role, or Modify role

To add a service:

1. In the **Services** window, click the **Add Service** button.

Tip

Alternatively, click **Add Service** in the **Actions** menu.

2. In the list of service templates in the **Add Service** dialog box, click the service template you want to add.
3. In the **Service Name** text box, enter the service name.
Set a service name that is unique within the resource group.
4. In the **Description** text box, enter a description of the service.
5. In the **Category** text box, enter the category name.
Specify a maximum of 256 characters, but do not specify control characters (\u0000 to \u001F and \u007F to \u009F). You can enter categories as a hierarchy by separating them with forward slashes (/). The maximum of hierarchical levels you can specify is 10. You must specify a value for each hierarchical level.
To assign multiple categories to the service, separate the category names with commas. However, you cannot specify the same category more than once. Also, you must specify values for each category.
You cannot precede or follow the hierarchy with a forward slash. Also, do not use commas, back slashes, and forward slashes in a category name.
6. Check the value in the **Resource Group for Service** list box, and select a resource group if you want to change the value.
Initially, the list box displays the resource group to which the user belongs.
7. Click the **Add Service** button.
8. In the **Information** dialog box, click the **OK** button.
9. In the **Service Definition** dialog box, check the service information and enter the required values in the service properties.
The properties you are required to enter depend on the service template.
If the **Preset Properties** list box appears, you can apply a set of property values appropriate for the user environment and mode of operation by selecting a name from the list and clicking the **Apply** button.
10. Click the **OK** button.

11. In the **Information** dialog box, click the **OK** button.

The service is added to the list of services in the **Services** window.

4.2 Editing services

The following describes how to edit a service that appears in the list of services in the **Services** window.

Who can perform this task:

Users in the Admin role, Develop role, or Modify role

To edit a service:

1. In the **Services** window, select the service you want to edit.

Important note

Because clicking the name of a service opens the **Submit Service** dialog box, click in the white area of the service name field to select the service.

2. Click the **Edit Service** button.
3. In the **Service Definition** dialog box, enter the service information and property information.
If the **Preset Properties** list box appears, select a preset property name, and then click the **Apply** button. This operation lets you apply a set of property values appropriate for the user environment and mode of operation.
4. Click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

The new service information and property information take effect.

You can check the edited service information by clicking the **Edit Service** button and viewing the information in the **Service Definition** dialog box.

4.3 Deleting services

You can delete services you have added to JP1/AO from the list of services in the **Services** window.

Criteria for deleting services:

There are no tasks in the Tasks list that were generated from the service you are deleting. You can, however, delete a service for which history entries exist in the history list.

Who can perform this task:

Users in the Admin role, Develop role, or Modify role

To delete a service:

1. In the **Services** window, select the service you want to delete.

You can select multiple services by holding down the **Ctrl** key and clicking. To select all services, click the **Select All** button.

Important note

Because clicking the name of a service opens the **Submit Service** dialog box, click in the white area of the service name field to select the service.

2. Click the **Delete Services** button.
3. In the **Delete Services** dialog box, review the service you want to delete, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The service is deleted from the list of services in the **Services** window.

4.4 Outputting (exporting) a list of services

You can output a list of services to a file in CSV format. Outputting a list of services is also called exporting a list of services. You can then use this list to verify the services that have been added to JP1/AO. A list of services allocated to resource groups associated with the specified user is output. Specify the user by using the `listservices` command with the `/user` option specified.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role who also have Administrator permissions for the OS

To output a list of services:

From the command prompt, execute the `listservices` command with `services` specified in the `/output` option.

A list of services is output as a CSV file to the location specified in the command.

5

Executing Services

This chapter describes how to execute services in JP1/AO.

5.1 Submitting services for immediate execution

This section describes how to submit a service for immediate execution. As soon as the user submits the service for execution, JP1/AO generates a task and processing begins immediately.

You can use the user interface or commands to submit a service for immediate execution.

Who can perform this task:

- To submit services for immediate execution from the user interface:
Users in the Admin role, Develop role, Modify role, or Submit role
- To submit services for immediate execution using a command:
Users in the Admin role, Develop role, Modify role, or Submit role who also have Administrator permissions for the OS

To submit a service for immediate execution from the JP1/AO user interface:

1. In the **Services** window, select the service you want to submit for execution, and then click the **Submit** button.

Tip

Alternatively, in the **Services** window, you can click the name of the service you want to submit for execution.

2. In the **Submit Service** dialog box, enter information about the task.
3. Check the property information, and enter the required values in the relevant fields.
The required property information depends on the service template.
4. In the **Schedule Type** list box, select **Now**.
5. Click the **Show Plan** button.
6. Review the information in the **Plan Summary** dialog box, and then click the **Submit** button.

JP1/AO generates the task, and processing begins immediately.

You can check the status of the task in the status column in the **Tasks** view of the **Tasks** window.

To submit a service for immediate execution using a command:

From the command prompt, execute the `submittask` command.

As soon as you submit the service for execution, JP1/AO generates a task and processing begins immediately.

You can check the status of the task in the status column in the **Tasks** view of the **Tasks** window.

5.2 Submitting services for execution at a specified time

This section describes how to submit services for execution at a specified time. JP1/AO generates a task as soon as the service is submitted for execution, but does not start processing the task until the scheduled start time.

You can use JP1/AO in a time zone in which daylight saving time is in effect.

Who can perform this task:

- When submitting a service for execution by specifying the date and time in the operation window
Admin role, Develop role, Modify role, or Submit role
- When submitting a service for execution by specifying the date and time using a command
Users who have the Admin role, Develop role, Modify role, or Submit role in addition to Administrators permission for the OS

To submit a service for execution by specifying the date and time in the operation window:

1. In the **Services** window, select the service you want to submit for execution, and then click the **Submit** button.

Tip

Alternatively, in the **Services** window, you can click the name of the service you want to submit for execution.

2. In the **Submit Service** dialog box, enter information about the task.
3. Check the property information, and enter the required values in the relevant fields.
The required property information depends on the service template.
4. In the **Schedule Type** list box, select **Later**. Enter the execution start date and time in **Schedule Starts On** and **Schedule Time**, respectively.
5. Click the **Show Plan** button.
6. Review the information in the **Plan Summary** dialog box, and click the **Submit** button.

JP1/AO generates a task which is placed in Waiting status.

In the **Status** column in the **Tasks** view of the **Tasks** window, make sure that the task is in Waiting status. The task begins processing at the scheduled start time.

To submit a service for execution by specifying the date and time using a command:

Start the command prompt, and execute the `submittask` command.

A task is generated when the service is executed, and processing enters Waiting status.

In the Status column of the **Tasks** view of the **Tasks** window, you can make sure the processing is in the Waiting status. The first processing will be executed at the specified time.

Related topics

- [1.5.3 Using JP1/AO in time zones affected by daylight saving](#)

5.3 Submitting services for recurring execution

Specify the date and time at which you want the service to start, and how frequently you want the service to recur. JP1/AO generates the task as soon as you submit the service for execution, but does not execute it until the scheduled start time. Additional tasks are generated and processed as the recurring schedule dictates.

You can use JP1/AO in a time zone in which daylight saving time is in effect.

Who can perform this task:

- When submitting a service for execution regularly in the operation window
Admin role, Develop role, Modify role, or Submit role
- When submitting a service for execution regularly by using a command
Users who have the Admin role, Develop role, Modify role, or Submit role in addition to Administrators permission for the OS

To submit a service for execution regularly in the operation window:

1. In the **Services** window, select the service you want to submit for execution, and then click the **Submit** button.

Tip

Alternatively, in the **Services** window, you can click the name of the service you want to submit for execution.

2. In the **Submit Service** dialog box, enter information about the task.
3. Check the property information, and enter the required values in the relevant fields.
The required property information depends on the service template.
4. In the **Schedule Type** list box, select **Recurring**, and enter the execution start date.
5. In the **Recurrence Pattern** list box, select the frequency at which execution of the service recurs.
6. Select the date and time of recurrence.
 - If you select **Daily**:
Enter the time at which the service recurs.
 - If you select **Weekly**:
Enter the day of the week and time of day at which the service recurs.
 - If you select **Monthly**:
Enter the day of the month and time of day at which the service recurs. You can schedule the service to execute at the end of each month by selecting the **Last day of the month** check box and entering the time of day at which execution of the service is to recur.
7. Click the **Show Plan** button.
8. Review the information in the **Plan Summary** dialog box, and then click the **Submit** button.

A task is generated and placed in **Waiting** status.

In the **Status** column in the **Tasks** view of the **Tasks** window, you can make sure the task is in **Waiting** status. The first of the series of tasks begins processing at the scheduled start time.

To submit a service for execution regularly using a command:

Start the command prompt, and execute the `submittask` command.

A task is generated when the service is executed, and processing enters the Waiting status.

In the Status column of the **Tasks** view of the **Tasks** window, you can make sure the processing is in the Waiting status. The first processing will be executed at the specified time.

Related topics

- [1.5.3 Using JP1/AO in time zones affected by daylight saving](#)

6

Managing Tasks

This chapter describes how to manage tasks in JP1/AO.

6.1 Checking the status of tasks executed by the logged-in user

The task summary area at the bottom of the main window summarizes the statuses of tasks executed by the logged-in user. In this area, you can see how many tasks are in the **Waiting**, **Waiting for Response**, **In Progress**, **Completed**, and **Failed** statuses.

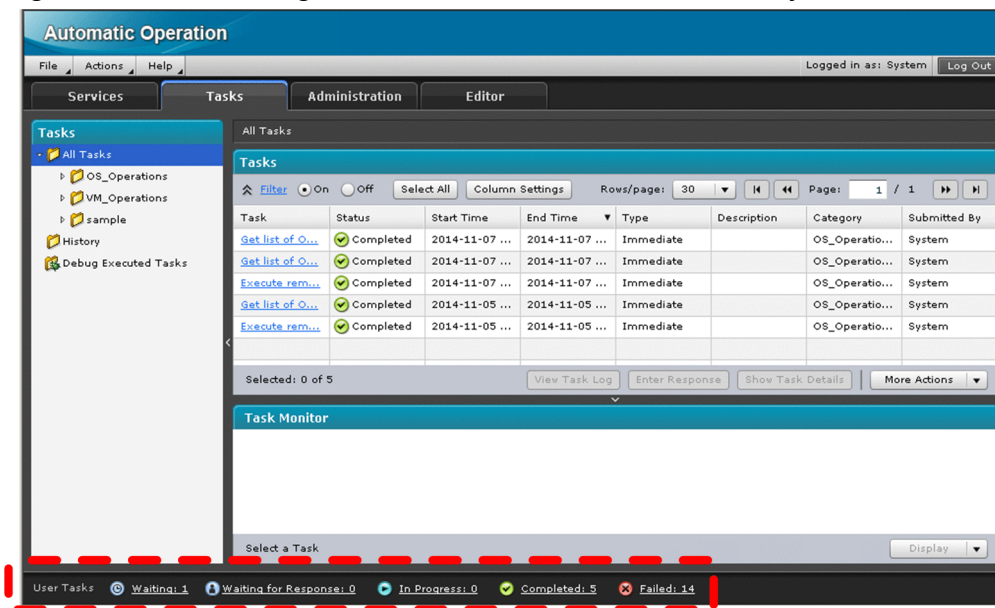
Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To check the status of tasks executed by the logged-in user:

1. Display the main window.
2. In the task summary area at the bottom of the main window, you can check the status of tasks and see how many tasks are in each status.

Figure 6–1: Checking task statuses in the task summary area



3. You can display a list of tasks in a particular status by clicking the status in the task summary area.

Related topics

- 1.6.10 Display format of task summary

6.2 Checking the status of all tasks

You can display a list of All Tasks statuses for which the user has reference permission.

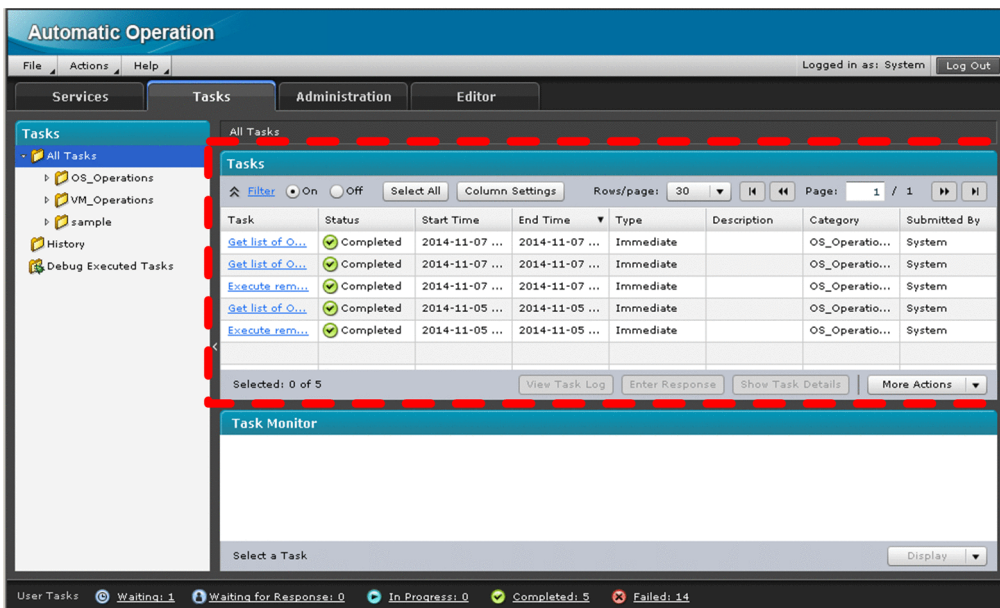
Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To check the status of all tasks:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. Check the status of tasks in the right pane (**Tasks** view) of the **Tasks** window.

Figure 6–2: Checking task statuses in the Tasks list



Tip

You can display detailed information about a task by clicking the name of the task in the **Tasks** view.

Related topics

- 1.6.12 Task statuses and status transitions

6.3 Checking the progress of a task

You can check the progress of a task in flow format or in a list. The procedure for checking the progress is described in the following subsections.

6.3.1 Checking the progress of tasks in flow format

You can check the processing status of a task for each step. You can view which steps of the running task have been processed. In the **Task Monitor** view, you can check all hierarchies of a task flow.

Note, however, that you can check the progress of a task in the **Task Monitor** view regardless of the JP1/AO version when a service template was created and imported.

Important note

You cannot display tasks restored by the `restoresystem` command in the **Task Monitor** view.

Tip

When all of the following conditions are met, if you check the progress of a task in flow format, repeated execution input values are displayed as null characters. As a result, the name indicating the repeated execution flow is displayed as an icon in *number-of-repetitions_* format.

- The task contains a repeated execution plug-in (repeated steps).
- After executing this task in JP1/AO version 10-10 or earlier, JP1/AO is upgraded.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

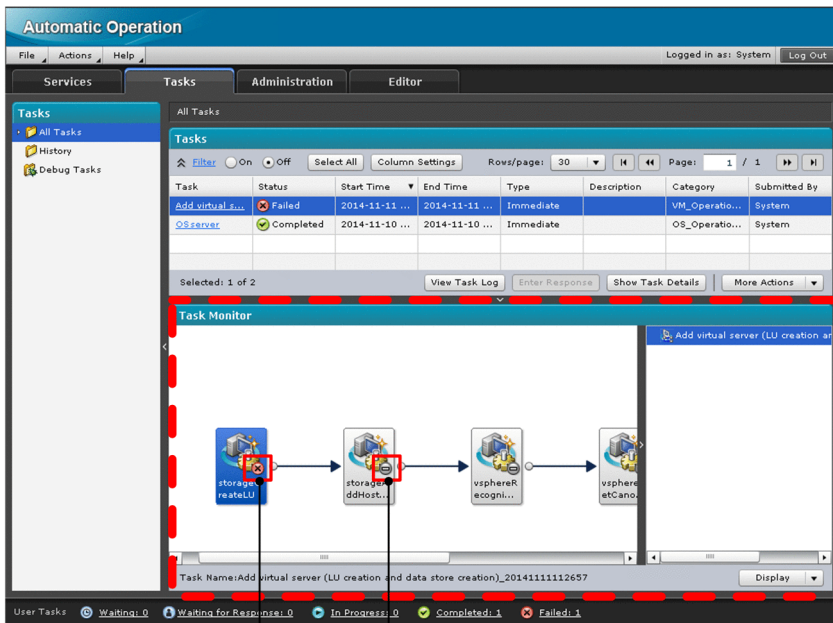
To check the progress of a task in flow format:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane of the **Tasks** window (**Tasks** view), select the line of the task for which you want to check progress.
3. In the **Task Monitor** view, check the progress of a task. The progress is displayed as an icon, indicating the status.

Tip

In the **Task Monitor** view, if you double-click a step icon, you can display the levels of the hierarchy under the steps in a flow view or tree view.

Figure 6–3: Display example of the **Task Monitor** view



The status of the step with the icon is Not Executed

The status of the step with the icon is Failed

Related topics

- [1.6.13 Step statuses](#)
- Step status icons in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*

6.3.2 Checking the progress of tasks in a list

Check the detailed progress of a task. You can check the overall progress of a task, and the progress of the individual steps. Note that you can display the list of steps defined for the top flow. Steps not listed in the top flow are not displayed.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To check the detailed progress of tasks in a list:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, click *task-name* for the task for which you want to check progress.

Tip

Alternatively, you can select the column corresponding to the task for which you want to check status, and then click the **Show Task Details** button.

3. Click **Step Details** at the bottom of the **Task Details** dialog box.
4. Check the overall progress of the task in **Step Information**.

5. Check the progress of individual steps in **Steps**.

Related topics

- [1.6.3 Managing task progress](#)
- [1.6.13 Step statuses](#)

6.4 Displaying task logs

In the **Task Log** dialog box, you can display and check the log created when you execute a task. The **Task Log** dialog box displays the content of the task log.

Task log data is output when the task enters one of the following statuses:

- In Progress
- Waiting for Response
- Abnormal Detection
- Terminated
- Completed
- Failed

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To display task log data:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. Select the row of a task for which you want to check log data.
3. Click the **View the Task Log** button at the bottom of the **Tasks** view or the **Task Details** dialog box.

You can perform the following operations in the **Task Log** dialog box:

- Updating task logs regularly and automatically
Select the **Update automatically** check box.
- Updating task logs manually
Click the **Update** button.
- Loading task logs

Tip

- When the **Update automatically** check box is selected, regardless of the task status, the task log is collected again, and the scroll bar in the **Task Log** dialog box slides down to the bottom.
- Specify the automatic update interval (in seconds) in the **Task Log** dialog box by using the `client.monitor.tasklog.ref resh.interval` key in the property file (`config_user.properties`).
- Specify the task log size (in KB) that is displayed in the **Task Log** dialog box by using the `client.monitor.tasklog.maxfilesize` key in the property file (`config_user.properties`).
- For details about how to display task logs for debug tasks, see the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

Related topics

- [6.5 Downloading task log files](#)
- [13.9.3 Task log details](#)

6.5 Downloading task log files

You can download and check the log created when you execute a task.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To download a task log file:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. Select the row of the task for which you want to check log data.
3. Click the **View the Task Log** button at the bottom of the **Tasks** view or the **Task Details** dialog box.
4. Click the **Download Log File** button at the bottom of the **Task Log** dialog box.
5. Specify the location to which to download the task log file.

Tip

- The size of a task log file you can download is the maximum value (in KB) for the log file size of the task specified in the property file (config_user.properties).
- For details about how to download a task log file for debug tasks, see the *Job Management Partner 1/ Automatic Operation Service Template Developer's Guide*.

Related topics

- [6.4 Displaying task logs](#)
- [13.9.3 Task log details](#)

6.6 Entering actions for tasks waiting for a response (entering responses)

This section describes how to enter a response when a task requires input (a decision or selection) by a user. Entering an action for a task in Waiting for Response status is called *entering a response*. When you enter a response, JP1/AO continues or stops the task according to the entered response.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To enter an action for a task waiting for a response:

1. In the right pane (**Tasks** view) of the **Tasks** window, select the task for which you want to enter a response, and then click the **Enter Response** button.

Tip

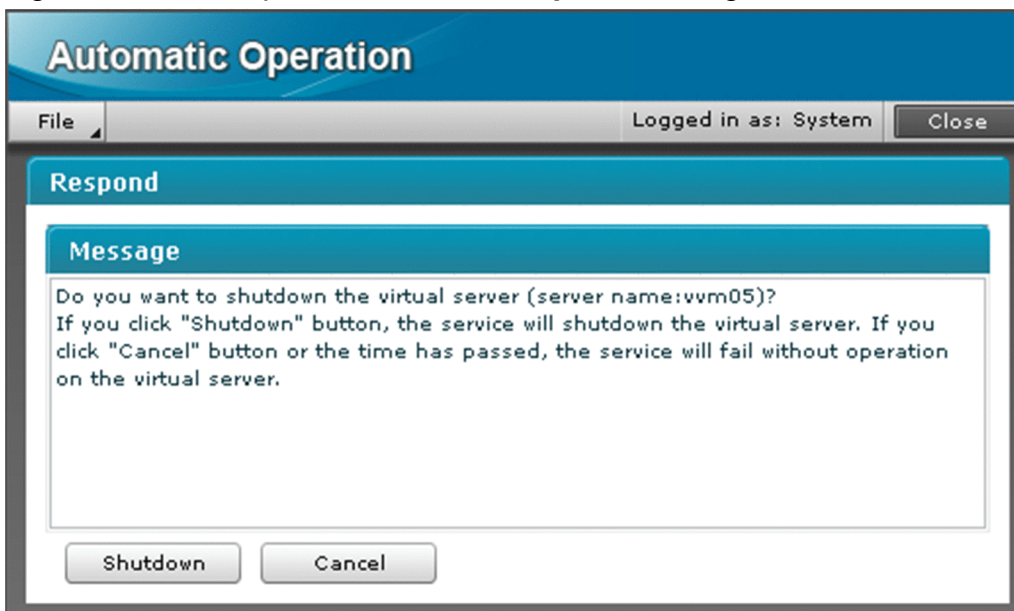
Alternatively, you can click the **Enter Response** button in the **Waiting for Response Task List** or **Task Details** dialog box.

You can also click the URL in the notification email sent when a task is waiting for a response, and log in from the **Login** window that opens.

2. Read the message in the **Enter Response** dialog box, and click the button associated with the operation you want to perform.
3. In the **Information** dialog box, click the **OK** button.

JP1/AO continues or stops the task according to the response you entered.

Figure 6–4: Example of the **Enter Response** dialog box





Important note

If JP1/AO stops processing the task while the **Enter Response** dialog box is open, an error occurs when you enter a response.

6.7 Suspending tasks (suspending schedules)

You can suspend the schedule of a waiting task. When you suspend a schedule, the task is put on hold until you resume the schedule.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To suspend a task:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task whose schedule you want to suspend. You can select multiple tasks by holding down the **Ctrl** key and clicking.

Important note

Because clicking the name of a task opens the **Task Details** dialog box, select tasks by clicking in the white area of the task name field.

3. From the **More Actions** menu, choose **Suspend Schedules**.
4. In the **Suspend Schedules** dialog box, verify the tasks you want to suspend, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

Tasks whose schedules are suspended are placed in Holding status.

You can check the status of tasks in the Status column of the **Tasks** view.

Related topics

- [6.8 Resuming suspended tasks \(resuming schedules\)](#)

6.8 Resuming suspended tasks (resuming schedules)

You can resume the schedule of a suspended task. When you resume a schedule, the associated task enters Waiting status. If you resume a schedule after the scheduled start time, the task is executed immediately.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To resume a suspended task:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task whose schedule you want to resume. You can select multiple tasks by holding down the **Ctrl** key and clicking.

Important note

Because clicking the name of a task opens the **Task Details** dialog box, select tasks by clicking in the white area of the task name field.

3. From the **More Actions** menu, choose **Resume Schedules**.
4. In the **Resume Schedules** dialog box, verify the tasks you want to resume, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

Tasks whose schedule you want to resume enter Waiting or Now Running status.

You can check the status of tasks in the Status column of the **Tasks** view.

Related topics

- [6.7 Suspending tasks \(suspending schedules\)](#)

6.9 Canceling tasks (canceling schedules)

You can cancel the schedule of a waiting task. When you cancel a schedule, the task enters Canceled status.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To cancel a task:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task whose schedule you want to cancel. You can select multiple tasks by holding down the **Ctrl** key and clicking.

Important note

Because clicking the name of a task opens the **Task Details** dialog box, select tasks by clicking in the white area of the task name field.

3. From the **More Actions** menu, choose **Cancel Schedules**.
4. In the **Cancel Schedules** dialog box, verify the tasks you want to cancel, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

Tasks whose schedule you cancel enter Canceled status.

You can check the status of tasks in the Status column of the **Tasks** view.

6.10 Stopping tasks (execution stop)

You can stop execution of, or forcibly stop running tasks. Each operation is described as follows:

- **Execution stop**
After the running steps finish, the task stops.
- **Forced stop**
The task stops without waiting for the running steps to complete.

Tip

You can also stop execution of, or forcibly stop debug tasks. For details about how to stop execution of, and forcibly stop debug tasks, see *Managing debug tasks in the Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

The subsequent subsections describe how to stop execution of, and forcibly stop running tasks.

6.10.1 Stopping tasks (execution stop)

This subsection describes how to stop execution of a task that is in progress. Stopped tasks enter Failed status.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To stop execution of a task:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task of which execution you want to stop.
You can select multiple tasks by holding down the **Ctrl** key and clicking.

Important note

Because clicking *task-name* opens the **Task Details** dialog box, select tasks by clicking in the white area except *task-name*.

3. From the **More Actions** menu, choose **Stop Tasks**.
4. In the **Stop Tasks** dialog box, verify the tasks you want to stop, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

Stopped tasks enter Failed status.

You can check the status of tasks in the Status column of the **Tasks** view. In addition to the task status, you can check the status, start time, and end time of steps in the **Task Details** dialog box, or in the **Task Monitor** view.

The start time and end time of tasks, information on executed plug-ins, and failure information can be checked in the task log or public log.

Important note

If a user stops execution of a task while the last plug-in of the task is running, the task terminates normally.

Related topics

- [1.6 Managing tasks](#)

6.10.2 Stopping tasks (forced stop)

This subsection describes how to forcibly stop a task that is in progress. Forcibly stopped tasks enter Failed status.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To forcibly stop a task:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task of which execution you want to forcibly stop. You can select multiple tasks by holding down the **Ctrl** key and clicking.

Important note

Because clicking *task-name* opens the **Task Details** dialog box, select tasks by clicking in the white area except *task-name*.

3. From the **More Actions** menu, choose **Forcibly Stop Tasks**.
4. In the **Forcibly Stop Tasks** dialog box, verify the tasks you want to forcibly stop, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

Forcibly stopped tasks enter Failed status.

You can check the status of tasks in the Status column of the **Tasks** view. In addition to the task status, you can check the status, start time, and end time of steps in the **Task Details** dialog box, or in the **Task Monitor** view.

The start time and end time of tasks, information on executed plug-ins, and failure information can be checked in the task log or public log.

Related topics

- [1.6 Managing tasks](#)

6.11 Redoing tasks

You can redo tasks by re-executing, or retrying them. Each operation is described as follows:

- **Re-execution**

You can re-execute stopped tasks (tasks enter in Completed, Failed, and Canceled status) by specifying a property value and another task ID.

- **Retry**

You can retry failed tasks. Use the same property value, and the same task ID to retry a task. Tasks are retried when tasks failed due to failures caused by inadequate environment, including temporary network disconnection.

You can retry tasks by performing either of the following methods:

- Retrying a task from a failed step
- Retrying a task from the step after the failed one

Important note

Identify and resolve the causes of a failure for the applicable step from the execution status and the result of each step in a task, and task log information before retrying tasks.

The subsequent subsections describe how to re-execute, and retry tasks.

6.11.1 Re-executing tasks

You can re-execute stopped tasks (tasks enter in Completed, Failed, and Canceled status). A task is re-executed with another task ID.

When a task is re-executed, its property value and description are inherited. Now is selected by default for Schedule.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To re-execute a stopped task:

1. In the left pane of the **Tasks** window, click **All Tasks** menu.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task you want to re-execute.
3. From the **More Actions** menu, choose **Resubmit**.

Tip

You can perform the same operation by clicking *task-name* or the **Show Task Details** button in the **Tasks** view to open the **Task Details** dialog box, and then clicking the **Resubmit** button.

Important note

After a task is generated, if the original service template is modified, an error might appear. If that happens, submit a service for execution in the **Submit Service** dialog box to set the property value instead of re-execution.

4. In the **Submit Service** dialog box, edit task information, as necessary.
The following information is set by default in the **Name** text box:
original-task-name_Resubmit
5. Check the property information, and edit the property value, as necessary.
6. From the **Schedule Type** list box, select the schedule.
By default, **Now** is selected.
7. Click the **Show Plan** button.
8. In the **Plan Summary** dialog box, check the settings, and then click the **Submit** button.

A task is generated, and processed according to the specified schedule.

You can check the generated task in the **Tasks** view.

Related topics

- [1.6 Managing tasks](#)
- [5.1 Submitting services for immediate execution](#)
- [5.2 Submitting services for execution at a specified time](#)
- [5.3 Submitting services for recurring execution](#)

6.11.2 Retrying tasks from failed steps

You can retry a task from the failed step. When a task is retried, the property value used when the task stopped last time is inherited, and the task can be retried with the same task ID from the failed step.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To retry a failed step:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task you want to retry.
3. From the **More Actions** menu, choose **Retry the Task From the Failed Step**.
4. In the **Retry the Task From the Failed Step** dialog box, click the **OK** button.

Tip

After a task is retried, you can check the retried history in the task log or public log.

Related topics

- [1.6 Managing tasks](#)

6.11.3 Retrying tasks from the step after the failed one

You can retry tasks from the step after the failed step of a failed task. When a task is retried, the property value used when the task stopped last time is inherited, and the task can be retried with the same task ID from the step after the failed one.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role

To retry a task from the step after the failed one:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select the task you want to retry.
3. From the **More Actions** menu, choose **Retry the Task From the Step After the Failed Step**.
4. In the **Retry the Task From the Step After the Failed Step** dialog box, click the **OK** button.

Tip

After a task is retried, you can check the retried history in the task log or public log.

Related topics

- [1.6 Managing tasks](#)

6.12 Moving tasks to the History list (archiving tasks)

You can archive tasks that have finished processing, by moving them to the History list. This operation is called archiving. Archived tasks no longer appear in the Tasks list, appearing in the History list instead.

Who can perform this task:

Users in the Admin role, Develop role, or Modify role

To move a task to the History list:

1. In the left pane of the **Tasks** window, click **All Tasks**.
2. In the right pane (**Tasks** view) of the **Tasks** window, select a task you want to archive.
You can select multiple tasks by holding down the **Ctrl** key and clicking. To select all tasks, click the **Select All** button.

Important note

Because clicking the name of a task opens the **Task Details** dialog box, select tasks by clicking in the white area of the task name field.

3. From the **More Actions** menu, click **Archive Tasks**.
4. Verify the tasks you want to archive in the **Archive Tasks** dialog box, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

The selected tasks are removed from the Tasks list.

By clicking the **History** menu in the left pane of the **Tasks** window, you can view the deleted tasks in the right pane (**Task Histories** view).

Tip

You can also configure JP1/AO to move tasks automatically to the History list, by setting retention periods and maximum retention counts in the property file (`config_user.properties`).

Related topics

- *Property file (`config_user.properties`) in the Job Management Partner 1/Automatic Operation Configuration Guide*

6.13 Deleting task histories

You can manually delete task histories that are no longer required. You can also configure JP1/AO to delete task histories automatically by setting the maximum number of task histories to keep in the property file (`config_user.properties`).

Who can perform this task:

Users in the Admin role, Develop role, or Modify role

To delete task histories:

1. In the left pane of the **Tasks** window, click **History**.
2. In the right pane (**Task Histories** view) of the **Tasks** window, select the task histories you want to delete.
You can select multiple task histories by holding down the **Ctrl** key and clicking. To select all histories, click **Select All**.
3. Click the **Delete Histories** button.
4. In the **Delete Task Histories** dialog box, verify the task histories you want to delete, and then click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

The task histories you selected are deleted from the History list.

Related topics

- *Property file (`config_user.properties`) in the *Job Management Partner 1/Automatic Operation Configuration Guide**

6.14 Outputting task lists (exporting tasks)

You can output task lists to a CSV file. Outputting a task list is called exporting tasks. By specifying a time range, you can narrow down the information that is output.

JP1/AO outputs a list of tasks allocated to resource groups associated with the user specified in the `/user` option of the `listtasks` command.

Who can perform this task:

Users in the Admin role, Develop role, Modify role, or Submit role who also have Administrator permissions for the OS

To export a list of tasks:

From the command prompt, execute the `listtasks` command with `tasks` specified in the `/output` option.

A list of tasks is output as a CSV file to the location specified in the command.

Tip

You can also use this procedure to export a list of task histories by executing the `listtasks` command with `histories` specified in the `/output` option.

6.15 Outputting detailed task information in a batch

You can output detailed task information including input and output properties information.

Who can perform this task:

Users in the Admin role who also have Administrator permissions for the OS

To output detailed task information in a batch:

Start the command prompt, and specify `taskdetails` for the `/output` option of the `listtasks` command for execution.

The detailed task information is output to the destination specified by the command.

6.16 Re-registering scheduled tasks and recurring tasks in a batch

You can re-register scheduled and recurring tasks with the same settings in a batch based on detailed task information output by using the `listtasks` command.

Who can perform this task:

Users in the Admin role who also have Administrator permissions for the OS

To re-register scheduled and recurring tasks in a batch:

Start the command prompt, and specify the `/reregister` and `/taskdetaildir` options for the `submittasks` command for execution. For the `/taskdetaildir` option, specify the folder where the detailed task information output by using the `listtasks` command is stored. Based on the detailed task information specified here, scheduled tasks and recurring tasks are re-registered in a batch.

7

Setting service share properties

This chapter describes how to set properties that are shared by multiple services. These properties are called service share properties.

7.1 Procedure for setting service share properties

The following describes how to set the service share property. By setting a value of a service share property, you can share, view, and update the value among multiple services.

Who can perform this task:

Users in the Admin role or Develop role

To set the service share property:

1. In the left pane of the **Administration** window, click **Service Share Properties**.
2. In the right pane (**Service Share Properties** view) of the **Administration** window, click the service share property you want to edit, and then click the **Set Service Share Property** button.
3. In the **Service Share Properties** dialog box, enter a property value, and then click the **OK** button.
The property values you can enter depend on the service share property you selected.
4. In the **Information** dialog box, click the **OK** button.

The new value is assigned to the service share property.

You can then check the value in the Value column in the **Service Share Properties** view.

8

Managing Users

This chapter describes how to manage users in JP1/AO.

8.1 Registering users in JP1/AO

The following describes how to register a user so that the user can use JP1/AO.

Who can perform this task:

Users with User Management permission

To register a user in JP1/AO:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, select **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), click the **Add User** button.
4. In the **Add User** dialog box (Users and Permissions), enter a user ID.
You can also enter a password, confirm the password, enter a full name, email address, and description of the user as needed.
5. Click the **OK** button.

The new user appears in the list of users in the **User List** view.

Important note

- Users in JP1/AO needed to be added to user groups, which in turn need to be allocated resource groups and roles.
- As the user authentication method, LDAP is set when Active Directory linkage is set for JP1/AO. If LDAP is not set, Internal is set by default.
You can change the user authentication method in the **Change Authentication Method** dialog box.

Related topics

- [8.9 Changing the user authentication method](#)

8.2 Setting of another user's information by an administrator

An administrator can edit the full name, email address, and description in the profile of another user.

Who can perform this task:

Users with User Management permission

To set the user information for another user as an administrator:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, select **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), click the user ID of the applicable user, and then click the **Edit Profile** button.
4. In the **Edit Profile** dialog box, edit the full name, email address, and description of the user, and then click the **OK** button.

The new user information is set.

You can check the new user information in the **User List** view.

8.3 Setting one's own user information

A login user can edit the full name, email address, and description in the user's own user information.

Who can perform this task:

All users

To set your own user information:

1. In the left pane of the **Administration** window, click **User Profile**.
2. In the **User Profile** window, click the **Edit Profile** button.
3. In the **Edit Profile** dialog box, edit your full name, your email address, and the description as needed, and then click the **OK** button.

The new user information is set.

You can check the new user information in the **User Profile** window.

8.4 Changing of another user's password by an administrator

An administrator can change the password of a user account other than his or her own. If the user account is being managed on an external authentication server, change the password on the external authentication server.

Who can perform this task:

Users with User Management permission

To change the password of another user as an administrator:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, click **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), click the user ID of the user whose password you want to change, and then click the **Change Password** button.
4. In the **Change Password** dialog box, enter the new password, and then enter the password again to confirm that you entered it correctly. Click the **OK** button.

The password is changed.

The user whose password you changed can now log in using the new password.

Important note

When using JPI/AO in a cluster system, if you change the password of the System account, you need to make the same change on every node in the cluster system.

8.5 Changing one's own password

A login user can change his or her own password. If your user account is being managed on an external authentication server, change the password on the external authentication server.

Who can perform this task:

All users

To change your own password:

1. In the left pane of the **Administration** window, click **User Profile**.
2. In the **User Profile** window, click the **Change Password** button.
3. In the **Change Password** dialog box, enter your current password and the new password, and then enter the new password again to confirm that you entered it correctly. Click the **OK** button.

The password is changed.

You can use the new password the next time you log in to JPI/AO.

8.6 Changing the User Management permission settings

The following describes how to assign or revoke User Management permission for individual users. A user with User Management permission can manage users in JP1/AO.

Who can perform this task:

Users with User Management permission

To change the User Management permission settings:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, click **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), click the user ID of the user whose permissions you want to change, and then click the **Change Permission** button.
4. In the **Change Permission** dialog box, change the permissions as needed and then click the **OK** button.

The User Management permission of the user you selected is changed.

You can make sure that the changes have taken effect by clicking the user ID of the user in the **User List** view.

Important note

- If you change the permission of a logged-in user, the user keeps his or her original permissions while logged in. The system administrator must instruct any such users to immediately log out and log back in.
- Users who manage and submit services in JP1/AO do so subject to the roles assigned to the user group to which they belong. These tasks are not controlled by User Management permission.
- A user with User Management cannot revoke his or her own permission. To revoke the permission of a user with User Management permission, log in to JP1/AO using the System account or another account with User Management permission.

8.7 Locking users

The following describes how to lock a user to prevent the user from accessing JP1/AO. When you lock a logged-in user, the user will no longer be able to continue operations in JP1/AO.

Who can perform this task:

Users with User Management permission

To lock a user:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, click **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), select the check box next to the user you want to lock, and then click the **Lock Users** button.
4. In the **Lock Users** dialog box, click the **OK** button.

The user you selected is locked.

You can check the status of the user (locked) in the **Status** column of the **User List** view.

8.8 Unlocking users

The following describes how to unlock a user. You can unlock users from the user interface or by using a command.

Who can perform this task:

From the user interface:

Users with User Management permission

Using a command:

Users who have Administrator permissions for the OS and User Management permission

To unlock a user from the user interface:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, click **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), select the check box next to the user you want to unlock, and then click the **Unlock Users** button.
4. In the **Unlock Users** dialog box, click the **OK** button.

To unlock a user by using a command:

1. From the command prompt, execute the `hcmdsunlockaccount` command as follows:

```
hcmdsunlockaccount /user user-ID /pass password
```

The user is no longer locked.

You can check the status of the user (*Active*) in the **Status** column of the **User List** view.

8.9 Changing the user authentication method

The following describes how to change the user authentication method:

Who can perform this task:

Users with User Management permission

To change the user authentication method:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, select **Users**.
3. In the right pane of the **Users and Permissions** window (**User List** view), select the check box next to the applicable user ID, and then click the **Change Authentication Method** button.
4. In the **Change Authentication Method** dialog box, select the user authentication method from the **Authentication** list box.
To authenticate users in JP1/AO, select **Internal**, in Active Directory, select **LDAP**.
5. In the **Change Authentication Method** dialog box, click the **OK** button.

The user authentication method has been changed.

Important note

If you change the authentication method of a user whose password is not managed in JP1/AO from **LDAP** to **Internal**, the user is locked automatically, and is no longer able to log in to JP1/AO. If you set a password for the user in JP1/AO, or change the authentication method back to **LDAP**, the user is unlocked.

Related topics

- [8.4 Changing of another user's password by an administrator](#)

8.10 Deleting users from JP1/AO

The following describes how to delete a registered user from JP1/AO.

Who can perform this task:

Users with User Management permission

To delete a user from JP1/AO:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, click **Users**.
3. In the right pane (**User List** view) of the **Users and Permissions** window, select the check box next to the user you want to delete, and then click the **Delete Users** button.
4. In the **Delete Users** dialog box, click the **OK** button.

The user is deleted from the **User List** view.

9

Managing Resource Groups

This chapter describes how to manage resource groups in JP1/AO.

9.1 Creating resource groups

This section describes how to create resource groups in which to group resources by category or other characteristics.

Who can perform this task:

Users in the Admin role

To create a resource group:

1. In the left pane of the **Administration** window, click **Resource Groups**.
2. In the right pane (**Resource Group** view) of the **Administration** window, click the **Create Resource Group** button.
3. In the **Create Resource Group** dialog box, enter a resource group name and, if needed, a description, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The resource group is registered in the list of resource groups in the **Resource Group** view.

After creating a resource group, assign it to a user group. When you assign a resource group to the user group, the users in that user group are able to access and work with the resources in the resource group.

Related topics

- [10.1 Creating user groups](#)

9.2 Editing resource groups

The following describes how to edit an existing resource group.

Who can perform this task:

Users in the Admin role

To edit a resource group:

1. In the left pane of the **Administration** window, click **Resource Groups**.
2. In the right pane (**Resource Group** view) of the **Administration** window, select the resource group you want to edit, and then click the **Edit Resource Group** button.
3. In the **Edit Resource Group** dialog box, edit the resource group name and the description as needed, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The new name and description are assigned to the resource group.

You can check the resource group you edited in the **Resource Group** view.

9.3 Deleting resource groups

The following describes how to delete resource groups.

Who can perform this task:

Users in the Admin role

To delete resource groups:

1. In the left pane of the **Administration** window, select **Resource Groups**.
2. In the right pane (**Resource Group** view) of the **Administration** window, select the resource group you want to delete, and then click the **Delete Resource Groups** button.
You can select multiple resource groups by holding down the **Ctrl** key and clicking.
3. In the **Delete Resource Groups** dialog box, click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The resource groups you selected are removed from the **Resource Group** view.

10

Managing User Groups

This chapter describes how to manage user groups in JP1/AO.

10.1 Creating user groups

This section describes how to create a user group whose members can log in to and use JP1/AO.

Who can perform this task:

- If you are adding resource groups when you create the user group:
Users in the Admin role who also have User Management permission
- If you are not adding resource groups when you create the user group:
Users who have User Management permission

To create a user group:

1. In the left pane of the **Administration** window, click **User Groups**.
2. In the right pane (**User Groups** tab) of the **Administration** window, click the **Create User Group** button.
3. In the **Create User Group** dialog box, enter a name and a description.
4. Click the **Add Users** button.
5. In the **Add Users** dialog box (**User Groups** view), select the users you want to add and then click the **OK** button.
6. In the **Create User Group** dialog box, click the **Add Resource Groups** button.
7. In the **Add Resource Groups** dialog box, select the resource groups you want to add, and then click the **OK** button.
8. In the **Create User Group** dialog box, click the **OK** button.
9. In the **Information** dialog box, click the **OK** button.

The user group is added to the **User Groups** tab of the **Administration** window.

Related topics

- [8.1 Registering users in JP1/AO](#)

10.2 Editing user groups

This section describes how to edit an editing user group. You can edit the user group name, the users who belong to the user group, and other properties.

Who can perform this task:

- If you are editing resource groups when you edit the user group:
Users in the Admin role who also have User Management permission
- If you are not editing resource groups when you edit the user group:
Users who have User Management permission

To edit a user group:

1. In the left pane of the **Administration** window, click **User Groups**.
2. In the right pane (**User Groups** tab) of the **Administration** window, select the user group you want to edit, and then click the **Edit User Group** button.
3. In the **Edit User Group** dialog box, edit the name, description, users, and resource groups as needed, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The new user group settings take effect.

You can check the new settings by clicking the name of the user group in the **User Groups** tab and then clicking the **Edit Resource Group** button.

Related topics

- [10.4 Assigning resource groups and roles to user groups](#)

10.3 Registering Active Directory groups linking with JP1/AO

When linking with Active Directory, if you want to link groups, register groups of Active Directory as user groups of JP1/AO.

Who can perform this task:

Users with User Management permission

To register Active Directory groups to link with JP1/AO:

1. In the left pane of the **Administration** window, click **Users and Permissions**.
2. In the left pane of the **Users and Permissions** window, select **Groups**.
3. In the right pane of the **Users and Permissions** window (**Groups** view), click *domain-name* to which the group you want to register belongs.
4. In the **Group List** view, click the **Add Groups** button.
5. In the **Add Groups** dialog box, enter the identification name for the group of Active Directory to link with JP1/AO in the **Distinguished Name** text box.
Enter the identification name according to RFC 4514.
6. If necessary, click the **Check DN** button.
Verification to check if the entered identification name is specified correctly, and if the identification name is registered in Active Directory.
7. Click the **OK** button.

The group of Active Directory to link with JP1/AO is registered.

10.4 Assigning resource groups and roles to user groups

This section describes how to assign resource groups and roles to selected user groups.

Tip

Assign resource groups and roles to Active Directory groups registered as user groups of JP1/AO. When doing so, perform the following procedure:

Tasks that must be completed beforehand:

- Create resource groups
- Create user groups

Who can perform this task:

Users in the Admin role who also have User Management permission

To assign resource groups and roles to a user group:

1. In the left pane of the **Administration** window, click **User Groups**.
2. In the right pane (**User Groups** tab) of the **Administration** window, select the user group to which you want to assign resource groups and roles, and then click the **Edit User Group** button.
3. In the **Edit User Group** dialog box, click the **Add Resource Groups** button.
4. In the **Add Resource Groups** dialog box, select the resource groups and roles you want to assign, and then click the **OK** button.
5. In the **Edit User Group** dialog box, click the **OK** button.
6. In the **Information** dialog box, click the **OK** button.

The resource groups and roles you selected are assigned to the user group.

You can check the resource groups and roles assigned to the user group in the **Edit User Group** dialog box.

10.5 Changing the user groups to which a user belongs

This section describes how to change the user groups to which a user belongs.

Who can perform this task:

Users with User Management permission

To change the user groups to which a user belongs:

1. In the left pane of the **Administration** window, click **User Groups**.
2. In the right pane (**User Groups** tab) of the **Administration** window, select the user whose user group affiliations you want to change, and then click the **Assign User Groups** button.
3. In the **Assign User Groups** dialog box, change the user groups to which the user belongs.
 - To assign the user to an additional user group:
In the **Available User Groups** area, select the user group to which you want to assign the user, and then click the **Add** button.
 - To remove a user from a user group:
In the **Selected User Groups** area, select a user group to which the user belongs, and then click the **Remove** button.
4. Click the **OK** button.
5. In the **Information** dialog box, click the **OK** button.

The user group affiliations of the user are changed. The user can now operate JP1/AO subject to the roles of the user groups to which he or she belongs.

You can view the new user group affiliations in the **User Group** column of the **Users** tab.

Important note

If you change the user group permissions for a logged-in user, that user retains his or her original permissions during the login session. For this reason, the system administrator must instruct any such users to immediately log out and log back in.

10.6 Deleting user groups

The following describes how to delete a user group from the JP1/AO system.

Who can perform this task:

Users with User Management permission

To delete a user group:

1. In the left pane of the **Administration** window, click **User Groups**.
2. In the right pane (**User Groups** tab) of the **Administration** window, select the user group you want to delete, and then click the **Delete User Groups** button.
You can select multiple user groups by holding down the **Ctrl** key and clicking.
3. In the **Delete User Groups** dialog box, verify the user groups you are about to delete, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The user groups you selected are removed from the list of user groups in the **User Group** tab.

Important note

You cannot delete user groups that have been assigned roles in a Hitachi Command Suite product. To delete such a user group, first remove the role from the user group in the Hitachi Command Suite product. You cannot use the JP1/AO interface to change roles assigned in Hitachi Command Suite products.

11

Managing Connection Destinations

This chapter describes how to manage the connection-destination hosts to which JP1/AO services connect to perform operations. JP1/AO manages these destinations as connection destinations.

11.1 Defining connection destinations

This section describes how to create a connection destination definition and register it in JP1/AO as a connection destination. Registering a connection destination in JP1/AO lets you restrict access to destination hosts based on the resource group to which a task belongs.

Who can perform this task:

Users in the Admin role or the Develop role

To create a connection destination:

1. In the left pane of the **Administration** window, select **Connection Destinations**.
2. In the right pane (**Connection Destination** view) of the **Administration** window, click the **Create Connection Destination** button.
3. In the **Create Connection Destination** dialog box, specify a type, destination, and resource group.
4. If you want to register authentication information for the connection destination, select **Set** in the **Authentication Information** list box, select a protocol, and enter a user ID and password.
If you do not want to register authentication information, select **Do not set** in the **Authentication Information** list box.
5. Click the **OK** button.
6. In the **Information** dialog box, click the **OK** button.

The connection destination is added to the list of destinations in the **Connection Destination** view.

Related topics

- [1.12.5 Entry format for connection destinations](#)

11.2 Editing the definition information for connection destinations

The following describes how to edit a connection destination. This procedure allows you to change the resources to which each resource group has access after JP1/AO becomes operational.

Who can perform this task:

Users in the Admin role or the Develop role

To edit the definition information for a connection destination:

1. In the left pane of the **Administration** window, click **Connection Destinations**.
2. In the right pane of the **Administration** window (**Connection Destinations** view), select the connection destination that you want to edit, and then click **Edit Connection Destination**.
3. In the **Edit Destination** dialog box, edit the type, destination, resource groups, and authentication information as needed, and then click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The new settings are applied to the definition of the connection destination.

You can check the new settings in the **Connection Destination** view.

Related topics

- [1.12.5 Entry format for connection destinations](#)

11.3 Deleting connection destinations

The following describes how to delete connection destinations.

Who can perform this task:

Users in the Admin role or the Develop role

To delete connection destinations:

1. In the left pane of the **Administration** window, click **Connection Destinations**.
2. In the right pane of the **Administration** window (**Connection Destinations** view), select the connection destinations that you want to delete, and then click the **Delete Connection Destinations** button.
You can select multiple connection destinations by holding down the **Ctrl** key and clicking.
3. In the **Delete Destinations** dialog box, click the **OK** button.
4. In the **Information** dialog box, click the **OK** button.

The connection destinations are deleted from the list of connection destinations in the **Connection Destination** view.

12

Maintenance

This chapter describes how to back up, restore, and maintain a JP1/AO system, start and stop services, and restore JP1/AO servers remotely by using back up files. If you are using the JP1/AO user interface when JP1/AO services resume, you need to log in again.

12.1 Backing up data in a JP1/AO system (non-cluster configuration)

Back up the configuration information and database information of JP1/AO and JP1/Base before you perform tasks such as migrating JP1/AO to a new host or performing database maintenance.

Important note

- If you leave too much time after backing up the JP1/Base data, the status of the JP1/AO database will have changed. This can lead to inconsistencies between the data in the JP1/AO database and the JP1/Base backup data. For this reason, back up JP1/AO and JP1/Base in quick succession.
- When you back up and restore data in a JP1/AO system, some aspects of the data do not survive the backup process. For example, some of the detailed task information (step lists and progress information) is lost, and some task statuses are changed.

You can output detailed task information by executing the `listtasks` command before backing up data. In addition, you can re-register scheduled tasks and recurring tasks as other tasks with the same settings in a batch by using the output detailed task information, and executing the `submittask` command after restoration.

- Make sure that sufficient free space is available on the disk on which the folder for backup files is located. As a general rule, the amount of free space should exceed the size of the backup files by 20 MB.

Who can perform this task:

Users who have Administrator permissions for the OS

To back up a JP1/AO system (non-cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
3. Back up the following JP1/Base configuration information and database. For details about the backup procedure, see *Backup and recovery* in the *Job Management Partner 1/Base User's Guide*.
 - Definition file
 - Common definition information
4. Execute the `backupsystem` command to back up the database and configuration information for JP1/AO.

Tip

The files below are not backed up by the `backupsystem` command. Back them up manually if necessary:

- SSL server certificate file for HTTPS connection
- Private key file for HTTPS connection
- Private keyfile for public key authentication

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

Data is backed up to the specified backup folder.

Related topics

- [1.13.1 Notes on backup and restoration](#)
- *Stopping services* in the *Job Management Partner 1/Base User's Guide*
- *Backup and recovery* in the *Job Management Partner 1/Base User's Guide*

12.2 Backing up data in a JP1/AO system (cluster configuration)

Back up the configuration information and database information of JP1/AO and JP1/Base before you perform tasks such as migrating JP1/AO to a new host or performing database maintenance.

Important note

- If you leave too much time after backing up the JP1/Base data, the status of the JP1/AO database will have changed. This can lead to inconsistencies between the current JP1/AO data and the JP1/Base backup data. For this reason, back up JP1/AO and JP1/Base in quick succession.
- When you back up and restore data in a JP1/AO system, some aspects of the data do not survive the backup process. For example, some of the detailed task information (step lists and progress information) is lost, and some task statuses are changed.
- Make sure that sufficient free space is available on the disk on which the folder for backup files is located. As a general rule, the amount of free space should exceed the size of the backup files by 20 MB.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To back up a JP1/AO system (cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Take the following services and scripts registered in the cluster software offline:
 - `stopcluster` command
 - HAutomation Engine *logical-host-name*
 - HAutomation Engine Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - Services of Hitachi Command Suite products
3. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
4. In the cluster software, take the registered HiRDB/ClusterService _HD0 service offline.
5. Disable failover of the services and scripts registered in the cluster software. In the cluster software, set J1/AO so that it does not restart if resources enter Failed status.
 - JP1/Base_*logical-host-name*
 - JP1/Base Event *logical-host-name*
 - HiRDB/ClusterService _HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*

- `stopcluster` command
 - Services of Hitachi Command Suite products
6. Back up the following JP1/Base configuration information and database information shown below. For details about the backup procedure, see *Backup and recovery* in the *Job Management Partner 1/Base User's Guide*.
- Definition file
 - Common definition information
7. Execute the `backupsystem` command to back up the database and configuration information for JP1/AO.

Tip

The files below are not backed up by the `backupsystem` command. Back them up manually if necessary:

- SSL server certificate file for HTTPS connection
- Private key file for HTTPS connection
- Private key file for public key authentication

8. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
9. Enable failover of the services and scripts registered in the cluster software and listed below.
In the cluster software, you can configure JP1/AO to restart resources when they enter Failed status on the current node, and to fail over the resources if they could not be restarted.
- JP1/Base_ *logical-host-name*
 - JP1/Base Event *logical-host-name*
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command
 - Services of Hitachi Command Suite products
10. Take the following services and scripts registered in the cluster software online:
- HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command
 - Services of Hitachi Command Suite products

Data is backed up to the specified backup folder.

Related topics

- [1.13.1 Notes on backup and restoration](#)
- *Backup and recovery* in the *Job Management Partner 1/Base User's Guide*

12.3 Restoring data in a JP1/AO system (non-cluster configuration)

After performing tasks such as replacing the hosts in a JP1/AO system or performing database maintenance, restore the JP1/AO and JP1/Base data that you backed up.

Important note

- When you back up and restore data in a JP1/AO system, some aspects of the data do not survive the backup process. For example, some of the detailed task information (step lists and progress information) is lost, and some task statuses are changed.

You can output detailed task information by executing the `listtasks` command before backing up data. In addition, you can re-register scheduled tasks and recurring tasks as other tasks (with the same settings) in a batch by using the output detailed task information and executing the `submittask` command after restoration.

- Execute the `backupsystem` command to create the backup data.
- Make sure that the following items on the host from which the backup was obtained and on the host to which the backup is being restored are consistent:

Installation folder path, host name[#], IP address, mappings of JP1 users to OS users, system locale

#

The host name need not be consistent if you are changing the host name of the JP1/AO server or you are restoring the information as part of a migration to an environment with a different host name.

Who can perform this task:

Users who have Administrator permissions for the OS

To restore a JP1/AO system (non-cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
3. Restore the JP1/Base configuration information and database information.
When you restore a JP1/AO system while replacing hosts, if JP1/AO on the origination host is version 10-00 or later, you do not need to perform this step.
4. Restore the JP1/AO configuration information and database information by executing the `restoresystem` command.

Tip

The files below are not restored by the `restoresystem` command. Relocate them manually if necessary.

- SSL server certificate file for HTTPS connection
- Private key file for HTTPS connection
- Private key file for public key authentication

Store the files for HTTPS connection in the location defined in the `httpsd.conf` file, and the files for public key authentication in the location defined in the property file (`config_user.properties`).

5. Reconfigure the following definition files to suit the environment to which the data is being restored.

These definition files are backed up but not restored.

- Configuration file for external authentication server linkage (`exauth.properties`)
- Security definition file (`security.conf`)
- Port number settings (`httpsd.conf`, `hssd.conf`)

The definition files are stored in the following folders:

- `backup-folder\HBase\base\conf`
- `backup-folder\HBase\base\httpsd.conf`

6. Enable HTTPS connection if it is used for communication between JPI/AO and the Web browser.

7. If you changed the number of the port used for communication between JPI/AO and the Web browser or the task-processing engine, reset the port number according to the procedure for changing port numbers.

8. Start the JPI/AO system by executing the `hcmdssrv` command with the `/start` option specified.

Data is restored to the specified host.

Related topics

- [1.13.1 Notes on backup and restoration](#)
- [1.13.3 Data that is restored](#)
- *Creating a JPI user in JPI/Base* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the host name of the JPI/AO server* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *JPI/AO system migration procedure (to an environment with a different host name or IP address)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Stopping services* in the *Job Management Partner 1/Base User's Guide*
- *Backup and recovery* in the *Job Management Partner 1/Base User's Guide*
- *Procedure for setting up the configuration file for external authentication server linkage* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Property file (config_user.properties)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Security definition file (security.conf)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to enable HTTPS connections between Web browsers and JPI/AO* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the port number* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

12.4 Restoring data in a JP1/AO system (cluster configuration)

After performing tasks such as replacing a host in a JP1/AO system or performing database maintenance, restore the JP1/AO and JP1/Base data you backed up.

Important note

- When you back up and restore data in a JP1/AO system, some aspects of the data do not survive the backup process. For example, some of the detailed task information (step lists and progress information) is lost, and some task statuses are changed.

Before backing up data, you can execute the `listtasks` command to output detailed task information. In addition, you can re-register scheduled tasks and recurring tasks (with the same settings) as other tasks in a batch, by using the output detailed task information and executing the `submittask` command after restoration.

- Execute the `restoresystem` command on the primary server (the server whose mode is set to online in the `cluster.conf` file).
- Execute the `backupsystem` command to create backup data.
- Make sure that the following attributes on the host from which the backup was obtained and on the host to which the backup is being restored are consistent:

Installation folder path, host name[#], IP address, JP1 users to OS users, and system locale

#

The host name need not be consistent if you are changing the host name of the JP1/AO server or you are restoring the information as part of a migration to an environment with a different host name.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To restore a JP1/AO system (cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Take the following services and scripts registered in the cluster software offline:
 - `stopcluster` command
 - HAutomation Engine *logical-host-name*
 - HAutomation Engine Web Service
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
 - Services of Hitachi Command Suite products
3. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
4. In the cluster software, take the registered `HiRDB/ClusterService_HD0` service offline.
5. Disable failover of the services and scripts registered in the cluster software listed below. Configure JP1/AO not to restart if resources enter Failed status in the cluster software.

- JP1/Base_ *logical-host-name*
 - JP1/Base Event *logical-host-name*
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command
 - Services of Hitachi Command Suite products
6. Restore the configuration information and database information for JP1/Base.
When restoring JP1/AO while replacing hosts, if JP1/AO on the origination host is version 10-00 or later, you do not need to perform this step.
7. Bring the shared disk on the active server online.
8. On the primary server, execute the `restoresystem` command to restore the database and configuration information for JP1/AO.

Tip

The following files are not restored by executing the `restoresystem` command. Relocate them manually if necessary.

- SSL server certificate file for HTTPS connection
- Private key file for HTTPS connection
- Private key file for public key authentication

Store the files for HTTPS connection in the location defined in the `httpsd.conf` file, and the files for public key authentication in the location defined in the property file (`config_user.properties`).

9. Shut down the JP1/AO system by executing the `hcmdssrv` command with the `/stop` option specified.
10. On the primary server, reconfigure the following definition files to match the environment to which the data is being restored.
These definition files are backed up but not restored.
- Configuration file for external authentication server linkage (`exauth.properties`)
 - Security definition file (`security.conf`)
 - Port number settings (`httpsd.conf`, `hssso.conf`)
- The definition files can be found in the following folders:
- `backup-folder\HBase\base\conf`
 - `backup-folder\HBase\base\httpsd.conf`
11. If you changed the port number used for communication between JP1/AO and the Web browser or the port number used to communicate with task-processing engine on the primary server, make the same changes again in the target environment by following the procedure for changing port numbers.

12. Enable HTTPS connection on the active server if HTTPS connection is used for communication between JPI/AO and the Web browser.
13. Perform steps 9 to 12 on the standby server.
14. Enable failover of the services and scripts listed below registered in the cluster software.
Configure the cluster software to restart resources on the current node if they enter Failed status, and to fail over the applicable resources if they could not be restarted.
 - JPI/Base_ *logical-host-name*
 - JPI/Base Event *logical-host-name*
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command
 - Services of Hitachi Command Suite products
15. Bring the following services and scripts registered in the cluster software online:
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command
 - Services of Hitachi Command Suite products

Data is restored to the specified host.

Related topics

- [1.13.1 Notes on backup and restoration](#)
- [1.13.3 Data that is restored](#)
- *Creating a JPI user in JPI/Base in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the host name of the JPI/AO server in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *JPI/AO system migration procedure (to an environment with a different host name or IP address) in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Backup and recovery in the Job Management Partner 1/Base User's Guide*
- *Procedure for setting up the configuration file for external authentication server linkage in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Property file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Security definition file (security.conf) in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the port number in the Job Management Partner 1/Automatic Operation Configuration Guide*

- *Procedure to enable HTTPS connections between Web browsers and JPI/AO in the Job Management Partner 1/ Automatic Operation Configuration Guide*

12.5 Database maintenance (non-cluster configuration)

To optimize the JP1/AO database, use the `hcmsdbtrans` and `ajsembdbroorg` commands to reorganize the database.

Important note

When a task is archived automatically, free segments of a database are reclaimed. Fragmentation that cannot be resolved by reclaiming free segments of a database can be resolved by reorganizing that database. Consider reorganizing a database when JP1/AO is stopped for regular maintenance, or once a year.

For details about how to reorganize a database, see *Database maintenance (non-cluster configuration)*.

For details about the time when tasks are archived automatically, see *Property file (config_user.properties)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*.

Tip

Commands beginning with `ajs` are stored in the storage location folder of the system file for the task processing engine. For details, see *List of folders* in the *Job Management Partner 1/Automatic Operation Configuration Guide*. Specify `AJSROOT1` for the `-F` option of the commands that will execute.

Who can perform this task:

Users who have Administrator permissions for the OS

To perform maintenance (non-cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Shut down the JP1/AO system by executing the `hcmsdssrv` command with the `/stop` option specified.
3. Start the database by executing the `hcmsdbsrv` command with the `/start` option specified.
4. Export the JP1/AO data by executing the `hcmsdbtrans` command with the following options specified:
 - `/export` option
 - `/workpath` option
Specify the path of the work folder.
 - `/file` option
Specify the path for the archive file.
5. Import the JP1/AO database by executing the `hcmsdbtrans` command with the following options specified:
 - `/import` option
 - `/type` option
Specify `Automation`.
 - `/workpath` option
Specify the path of the work folder.

- `/file` option

Specify the path of the archive file.

6. Start the HAutomation Engine Database _JF0 service in the service manager.

7. Execute the `ajsembdbstart` command to start the task processing engine database.

8. Execute the `ajsembdbreclaim` command to reclaim free segments.

```
ajsembdbreclaim -m scheduler -F AJSROOT1
```

9. Execute the `ajsembdbbrorg` command to reorganize the database. Secure the required free space in the folder that will be specified for the `-d` option of the `ajsembdbbrorg` command, and then execute the `ajsembdbbrorg` command twice in the following order:

```
1. ajsembdbbrorg -k unld -F AJSROOT1 -d arbitrary-folder#
```

```
2. ajsembdbbrorg -k reld -F AJSROOT1 -d arbitrary-folder#
```

#

To use the data obtained using `ajsembdbbrorg -k unld` to execute `ajsembdbbrorg -k reld`, specify the two folders identically.

Important note

If an error occurs during execution of `ajsembdbbrorg -k unld` and a file is created, do not use the file to execute `ajsembdbbrorg -k reld`. If you do so, the database might be corrupted.

10. Start the JP1/AO system by executing the `hcmdssrv` command with the `/start` option specified.

The JP1/AO database and the task processing engine database are reorganized.

Important note

If the database is damaged and cannot be repaired by the `restoresystem` and `hcmdsdbtrans` commands, use the `hcmdsdbrepair` command to restore the database.

Related topics

- [1.6.9 Archiving tasks and removing histories automatically](#)
- *ajsembdbbrorg* command in the *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1*

12.6 Database maintenance (cluster configuration)

To optimize a JP1/AO database, execute the `hcmsdbtrans` and `ajsembdbroorg` commands to reorganize the database.

Important note

When a task is archived automatically, free segments of a database are reclaimed. Fragmentation that cannot be resolved by reclaiming free segments of a database can be resolved by reorganizing that database. Consider reorganizing the database when JP1/AO is stopped for regular maintenance, or once a year.

For details about how to reorganize a database, see *Database maintenance (non-cluster configuration)*.

For details about the time when tasks are archived automatically, see *Property file (config_user.properties)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*.

Tip

Commands beginning with `ajs` are stored in the storage location folder of the system file for the task processing engine. For details, see *List of folders* in the *Job Management Partner 1/Automatic Operation Configuration Guide*. Specify `AJSROOT1` for the `-F` option of the commands that will execute.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To perform a database maintenance (cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Take the following services and scripts registered in the cluster software offline:
 - `stopcluster` command
 - HAutomation Engine *logical-host-name*
 - HAutomation Engine Web Service
 - Services of Hitachi Command Suite products
 - HiRDB/ClusterService_HD0
 - HBase Storage Mgmt Web Service
 - HBase Storage Mgmt Common Service
3. Start the database by executing the `hcmsdbsrv` command with the `/start` option specified.
4. Export the JP1/AO database by executing the `hcmsdbtrans` command with the following options specified:
 - `/export` option
 - `/workpath` option
Specify the path of the work folder.
 - `/file` option

Specify the path for the archive file.

5. Import the JP1/AO data by executing the `hcmdsdbtrans` command with the following options specified:

- `/import` option
Specify `Automation`.
- `/type` option
Specify `Automation`.
- `/workpath` option
Specify the path of the work folder.
- `/file` option
Specify the path of the archive file.

6. In the service manager, start HAutomation Engine Database `_JF1`.

7. Start the database of the task processing engine by executing the `ajsembdbstart` command with the following option specified:

- `-id` option
Specify `_JF1`.

8. Execute the `ajsembdbreclaim` command to reclaim free segments.

```
ajsembdbreclaim -m scheduler -F AJSCLUSTER -mh logical-host-name
```

9. Execute the `ajsembdbbrorg` command to reorganize the database.

Secure the required free space in the folder that will be specified for the `-d` option of the `ajsembdbbrorg` command, and then execute the `ajsembdbbrorg` command in the following order:

1. `ajsembdbbrorg -k unld -F AJSCLUSTER -mh logical-host-name -d arbitrary-folder#`
2. `ajsembdbbrorg -k reld -F AJSCLUSTER -mh logical-host-name -d arbitrary-folder#`

To use the data obtained using `ajsembdbbrorg -k unld` to execute `ajsembdbbrorg -k reld`, specify the two folders identically.

Important note

If an error occurs during execution of `ajsembdbbrorg -k unld` and a file is created, do not use the file to execute `ajsembdbbrorg -k reld`. If you do so, the database might be corrupted.

10. Stop the database by executing the `hcmdsdbsrv` command with the `/stop` option specified.

11. Bring the following services and scripts registered in the cluster software online:

- `stopcluster` command
- HAutomation Engine *logical-host-name*
- HAutomation Engine Web Service
- HBase Storage Mgmt Web Service
- HBase Storage Mgmt Common Service
- Services of Hitachi Command Suite products

- HiRDB/ClusterService_HD0

The JP1/AO database and the task-processing engine database are reorganized.

Important note

If the database is damaged and cannot be repaired by the `restoresystem` and `hcmsddbtrans` commands, use the `hcmsdbrepair` command to restore the database.

Related topics

- [1.6.9 Archiving tasks and removing histories automatically](#)
- *ajsembdborg* command in the *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1*

12.7 Starting a JP1/AO system (non-cluster configuration)

This section describes how to start a JP1/AO system. Use the `hcmdssrv` command, not Service Control Manager, to start a system. If you use Service Control Manager, the system might fail to start.

Who can perform this task:

Users who have Administrator permissions for the OS

To start a JP1/AO system (non-cluster configuration):

From the command prompt, execute the `hcmdssrv` command with the `/start` option specified.

The JP1/AO system starts.

Important note

You can use the `/server AutomationWebService` option when the Common Component services are already running and the JP1/AO service is the only service you are starting. When starting JP1/AO in the course of day-to-day operation, start all services with this option omitted.

12.8 Starting a JP1/AO system (cluster configuration)

This section describes how to start a JP1/AO system. Bring services registered in the cluster software online within the software. Do not start the services directly.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To start a JP1/AO system (cluster configuration):

In Failover Cluster Manager, right-click the resource group that contains the JP1/AO service, and click **Bring this service or application online**.

The JP1/AO system starts.

12.9 Stopping a JP1/AO system (non-cluster configuration)

This section describes how to stop a JP1/AO system. Use the `hcmdssrv` command, not Service Control Manager, to stop the services. If you use Service Control Manager, the services might fail to stop.

Who can perform this task:

Users who have Administrator permissions for the OS

To stop a JP1/AO system (non-cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. From the command prompt, execute the `hcmdssrv` command with the `/stop` option specified.

The JP1/AO system stops.

Important note

You can use the `/server AutomationWebService` option when the Common Component services are running and the JP1/AO service is the only service you are stopping. When stopping JP1/AO in the course of day-to-day operation, stop all services with this option omitted.

12.10 Stopping a JP1/AO system (cluster configuration)

This section describes how to stop a JP1/AO system. Take the services registered in the cluster software offline within the cluster software. Do not stop the services directly.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To stop a JP1/AO system (cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Bring the following services and scripts registered in the cluster software online:
 - JP1/Base_ *logical-host-name*
 - JP1/Base Event *logical-host-name*
 - HiRDB/ClusterService _HD0
 - HBase Storage Mgmt Common Service
 - HBase Storage Mgmt Web Service
 - HAutomation Engine Web Service
 - HAutomation Engine *logical-host-name*
 - `stopcluster` command

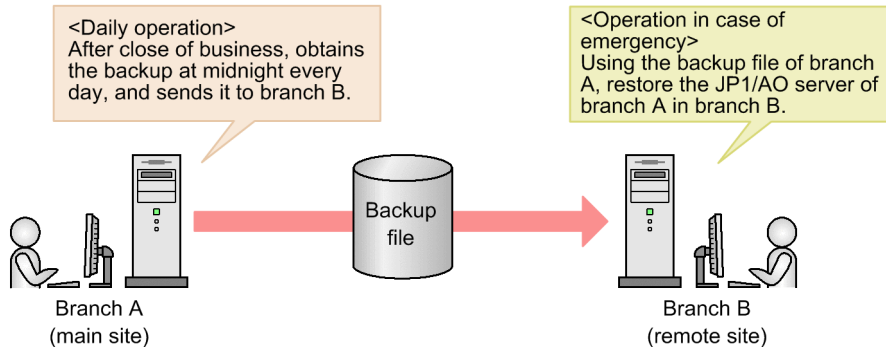
The JP1/AO system is now stopped.

12.11 Restoring JP1/AO servers remotely by using backup files

You can restore JP1/AO servers remotely by using backup files, even if a JP1/AO server stops for any reason. You can use this method for disaster recovery when a large disaster or system failure occurs.

See the following figure for details.

Figure 12–1: Example of restoring a JP1/AO server remotely by using backup files



Branch A, which is the main site, obtains the backup file after close of business at midnight every day, and sends it to branch B, which is a remote site. Branch B always retains the backup file of branch A created at midnight on the previous day. Because of this, if a disaster occurs in branch A and its JP1/AO server stops, the JP1/AO server can be restored in branch B from the backup file created at midnight on the previous day.

The procedure for restoring the JP1/AO server remotely by using the backup file is described below.

Prerequisite conditions

- The following items must match between the JP1/AO server in the main site and the JP1/AO server in the remote site:
 - System locale
 - JP1 user settings used in JP1/AO (permissions and uses of the mapped OS)
 - Versions of JP1/Base
 - Installation destination folder for JP1/Base
 - Versions of JP1/AO
 - Installation folder of JP1/AO
 - If Hitachi Command Suite products are installed, the environment of the Hitachi Command Suite products (configuration, versions, and revisions)
 - When public key authentication is used for connection with the target device, the storage location of the private key file

Note that the key can be allocated by the following methods:

 - Allocating the same key for the main site and a remote site
Send and allocate the private key file created in the main site to the remote site.
 - Allocating different keys in the main site and the remote site
Create separate keys for the main site and a remote site, and then allocate the corresponding public key file to the device to be used.
- The cluster environment is not constructed
- No update programs from versions 10-00 have been installed after the upgrade

Flow of restoring JP1/AO servers remotely by using the back-up file:

The following figure explains the flow for restoring the JP1/AO server in a remote site by using the backup file of the main site.

Table 12–1: Flow of restoring JP1/AO servers remotely by using the backup file

Timing	Main site	Remote site
During normal operation	Backs up data.#	--
	Sends the backed up file to a remote site.	--
When a disaster or failure occurs	--	Uses the latest backup file to restore the JP1/AO server in the main site.

Legend:

--: N/A

#

We recommend you back up data regularly and automatically.

Procedure during normal operation

Obtain the latest backup file of the main site, and send it to a remote site.

1. Obtain the latest backup file of the main site.

For details about how to obtain the backup file of JP1/AO servers, see [12.1 Backing up data in a JP1/AO system \(non-cluster configuration\)](#).

Note, however, that you do not need to perform the procedure for backing up JP1/Base settings or database information.

2. Send the obtained backup file of the main site to a remote site.

Tip

- You cannot back up the files below by the `backupsystem` command. If you intend to use the same file in the main site and a remote site, back up data manually when necessary, and send it to the remote site.
 - SSL server certificate file for HTTPS connection
 - Private key file for HTTPS connection
 - Private key file for public key authentication

You can use different files in the main site and a remote site. In that case, back up or create the above files separately in the main site and the remote site.

Procedure when a disaster or failure occurs

Use the latest backup file of the main site in the remote site to restore the JP1/AO server in the main site.

Tip

If the following settings for the JP1/AO servers in the main site and the remote site are the same, you do not need to perform steps 4 through 6:

- Configuration file for external authentication server linkage (exauth.properties)
- Security definition file (security.conf)
- Port number settings (httpsd.conf, hssso.conf)
- HTTPS connection settings (httpsd.conf)
- Number of the port between JP1/AO and the Web browser
- Number of the port used for communication between JP1/AO and the task-processing engine

1. In the remote site, make sure there is no task in In Progress, Waiting for Response, Abnormal Detection, or Terminated status. If there is such a task, stop execution of the task, or wait until it enters Completed or Failed status.
2. When the JP1/AO system is running, execute the `hcmdssrv` command with the `/stop` option specified to stop the JP1/AO system.
3. Execute the `restoresystem` command to restore settings or database information of JP1/AO in the main site.

Tip

You cannot restore the files below by using the `restoresystem` command. If you intend to use the same file in the main site and a remote site, reallocate it manually when necessary.

- SSL server certificate file for HTTPS connection
- Private key file for HTTPS connection
- Private key file for public key authentication

Store the files for HTTPS connection in the location defined in the `httpsd.conf` file, and the files for public key authentication in the location defined in the property file (`config_user.properties`).

4. Reset the definition files below according to the remote site environment.
You can back up the following definition files by using the `backupsystem` command, but cannot restore by using the `restoresystem` command.
 - Configuration file for external authentication server linkage (exauth.properties)
 - Security definition file (security.conf)
 - Port number settings (httpsd.conf, hssso.conf)
 - HTTPS connection settings (httpsd.conf)
 The definition files are stored in the following folders:
 - `backup-destination-folder\HBase\base\conf`
 - `backup-destination-folder\HBase\base\httpsd.conf`
5. Specify HTTPS connection settings if necessary.
6. If you have changed the default port number settings listed below, reset them according to the procedure for changing the port number:
 - Number of the port used for communication between JP1/AO and the Web browser
 - Number of the port used for communication between JP1/AO and the task-processing engine
7. Execute the `hcmdssrv` command with the `/start` option specified to start the JP1/AO system.

8. Execute the following command in the command prompt:

- `set JP1_USERNAME=JP1-user-to-use-in-JP1/AO` (the value for shared built-in service property *JP1-user-name*)
- `ajsagtalt -a loop -s host-name-in-remote-site`
- `ajsagtalt -a userResponse -s host-name-in-remote-site`

Tip

Commands beginning with `ajs` are stored in the storage destination folder of the system file in the task-processing engine. For details, see *List of folders* in the *Job Management Partner 1/Automatic Operation Configuration Guide*.

9. Execute the `hcmdschgurl` command to update the URL information according to the remote site environment.

The JP1/AO server of the main site is restored in the remote site.

Related topics

- *Procedure for setting up the configuration file for external authentication server linkage* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Security definition file (security.conf)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to enable HTTPS connections* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the port number* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to change the URL* in the *Job Management Partner 1/Automatic Operation Configuration Guide*
- *Procedure to set public key authentication for SSH connections* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

13

Troubleshooting JP1/AO

This chapter describes how to deal with issues that arise when using JP1/AO to automate aspects of an IT system. It also describes, in detail, the log data required to identify and resolve issues.

13.1 Types of problem

Refer to the troubleshooting method for the type of problem you are trying to resolve, as listed in the table below.

Table 13–1: Types of problem

Problem type	Troubleshooting method
A running task fails	13.2 When a running task fails
Taking time to complete tasks	13.3 Taking time to complete tasks
A task does not end	13.4 When a task does not end
Public key authentication with connection destinations fails	13.5 Public key authentication with connection destinations fails
You cannot access the JP1/AO GUI	13.6 When you cannot connect to the JP1/AO GUI
You cannot log in to JP1/AO	13.7 When you cannot log in to JP1/AO
JP1/AO will not start	13.8 When JP1/AO will not start

13.2 When a running task fails

If a task being executed fails, resolve the issue that caused the failure, and then submit the task for execution again. You can re-submit tasks by re-executing or retrying them.

Preparation

1. Select the failed task in the **Tasks** view.
2. Check the failed steps in the **Task Monitor** view.
In the **Steps** view of the **Task Details** dialog box, check the return value of the failed step.
3. Click the **View Task Log** button to check the task log.[#]
If either of the following cases applies, the JP1 user might not have sufficient permission.
 - The KNAE00216-E message appears and you cannot obtain log data for the task.
 - In the **Steps** view of the **Task Details** dialog box, the return value of the applicable step shows 66.Set the necessary JP1 user permissions, and then configure the execution agents manually. For setting details, see *What to do if an attempt to set execution agents for the task processing engine fails in the Job Management Partner 1/Automatic Operation Configuration Guide*.
4. From the information related to plug-in definitions in the log data, identify which plug-in failed.
5. In the task log, identify the cause of the problem from the return value of the plug-in.
For details about the return values of the content plug-in, see *Return values of content plug-ins in the Job Management Partner 1/Automatic Operation Service Template Developer's Guide* to take action according to the cause of the failure. For details about the return values of the basic plug-in, see the related topics section for each plug-in in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.
6. Take action according to the error messages and exception details in the task log.
7. Review the requirements for the service template, and make sure that your environment fulfills the requirements.
You can find the requirements for specific service templates in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.
8. After eliminating the cause of the problem, resubmit the failed task.

#

You can download the task log file by clicking the **Download Log File** button in the **task log** or **Task Details** dialog box.

Related topics

- [6.11 Redoing tasks](#)
- [13.9.3 Task log details](#)
- *What to do if an attempt to set execution agents for the task-processing engine fails in the Job Management Partner 1/Automatic Operation Configuration Guide*
- *Job Management Partner 1/Automatic Operation Messages*

13.3 Taking time to complete tasks

When using JP1/AO in an environment in which you cannot connect to an external network, you can configure the JP1/AO server to disable the Authenticode signature feature. By doing so, the time required until a plug-in starts execution, and the time required to complete a task can be reduced.

Related topics

- Settings in an environment where external networks cannot be connected in the *Job Management Partner 1/Automatic Operation Configuration Guide*

13.4 When a task does not end

When the following conditions exist, commands executed on a remote machine fail to stop executing. As a result, some tasks might remain in In Progress status.

- The OS of the remote machine is UNIX
- The command line executed on the remote machine contains non-ASCII characters
- The criteria for executing a command line that contains non-ASCII characters were not met

If a command executed remotely under these conditions fails to stop, check the processing of running steps and plugins in the **Task Monitor** view or the task log. After making sure that stopping the running task does not cause a problem, forcibly stop it.

Related topics

- [6.10.2 Stopping tasks \(forced stop\)](#)
- *Prerequisites for executing command lines containing non-ASCII characters in UNIX* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*

13.5 Public key authentication with connection destinations fails

If public key authentication with the connection destination fails, save the following information, and make sure there is no problem:

- Public key files
- Private key files
- Passphrases for private keys

Procedure

Use an SSH client product supporting public key authentication, check if you can perform authentication by using the user ID, private key, and pass phrase of the target device set for the JP1/AO server.

If the authentication fails, settings for the public key, private key, pass phrase corresponding to the private key, or SSH server might contain a problem. In this case, recreate a key, or review the SSH server settings.

If you cannot solve the problem, contact the Support Center.

13.6 When you cannot connect to the JP1/AO GUI

If you are unable to connect to the JP1/AO GUI, follow the procedure below.

Procedure

1. Check whether JP1/AO is running as a result of executing the `hcmdssrv` command with the `/status` option specified.
2. If the HAutomation Engine Web Service and HBase Storage Mgmt Common Service are running but the HBase Storage Mgmt Web Service is not, a port number conflict might have occurred. Check the Windows event log.
3. If the event log contains the following entry, review the port number settings used by the JP1/AO server:

Table 13–2: Log entry

Parameter	Content
Level	Error
Source	HitachiWebServer
Message	The service named HBase Storage Mgmt Web Service reported the following error: >>> (OS 10048)Only one usage of each socket address (protocol/network address/port) is normally permitted. : make_sock: could not bind to address [::]:[<i>duplicate-port-number</i>]

13.7 When you cannot log in to JP1/AO

If a user is unable to log in to JP1/AO, review the settings by doing the following:

- Check whether the user ID and password are specified correctly.
- Check whether the account is registered as a JP1/AO user.[#]
- Check whether a resource group and role have been assigned to the user group to which the user belongs.[#]
- Check whether the user account is locked.[#]

#

These tasks require User Management permission. Ask a user with User Management permission to check for you.

If the **Login** window does not appear, see [13.8 When JP1/AO will not start](#).

13.8 When JP1/AO will not start

If you are unable to start JP1/AO, follow the procedure below:

Procedure when the Login window does not appear

1. Check whether the JP1/AO services are running by executing the `hcmdsrv` command with the `/status` option specified.
If the JP1/AO services are not running, start the services.
2. Use your Web browser to check the status of the connection with the JP1/AO server.
If a firewall is in place, configure the firewall to allow traffic by JP1/AO.
3. Make sure that the Web browser and version of Adobe Flash Player on your system are compatible with JP1/AO.
For details on the Web browsers and versions of Adobe Flash Player supported by JP1/AO, see the JP1/AO release notes.
4. Review the log entries and take action according to the contents of the error messages.
5. If there are no error messages in the log data, or you are still unable to resolve the problem despite following the procedure above, execute the `hcmdsgetlogs` command to acquire log data and then contact the system administrator.

Procedure when JP1/AO does not start

1. Make sure that sufficient memory, disk space, and other resources are available on the JP1/AO server.
2. Make sure that JP1/AO is installed on supported hardware running a supported operating system.
For details on the hardware and operating systems that JP1/AO supports, see the JP1/AO release notes.
3. Review the log entries and take action according to the contents of the error messages.
4. If there are no error messages in the log data, or you are still unable to resolve the problem despite following the procedure above, execute the `hcmdsgetlogs` command to acquire log data and then contact the system administrator.

Related topics

- The manual *Job Management Partner 1/Automatic Operation Messages*
- [13.9 Detailed description of log information](#)

13.9 Detailed description of log information

JP1/AO outputs three types of log information as it operates:

- Task logs

Task log information is created for individual tasks executed in the JP1/AO system. JP1/AO generates task log entries that report when tasks start and stop, and entries containing information about called plug-ins and error information.

You can view or download task log data in the **Tasks** view, **Task Details** dialog box, and **Debug-Tasks** view.

- Integrated trace log and event log

Information about the system starting and stopping and errors that occurred in the system are output to the integrated trace log and event log.

- Public log

Messages output by JP1/AO, including messages output to the integrated trace log and event log and messages about problems that occurred in JP1/AO functionality, are output to the public log.

Related topics

- [13.9.3 Task log details](#)
- [13.9.4 Integrated trace log and event log details](#)
- [13.9.5 Public log details](#)

13.9.1 Format of log entries

JP1/AO outputs log information in the following format:

Figure 13–1: Format of log information

Serial number	Date	Time	rsvd	Program name	pid	tid	ID	Event type	Message text	Linefeed code
---------------	------	------	------	--------------	-----	-----	----	------------	--------------	---------------

The following table lists and describes the contents of log information output by JP1/AO.

Table 13–3: Contents of log information

No.	Item	Description	Length
1	Serial number	The serial number of the message.	4 bytes
2	Date	The date on which the message was output (in the format yyyy/mm/dd).	10 bytes
3	Time	The time at which the message was output (in the format hh:mm:ss:xxx, where xxx indicates milliseconds).	12 bytes
4	rsvd	A reserved space.	4 bytes
5	Program name	The name of the program. If the program name is longer than 16 characters, an abbreviated but recognizable form of the product name is used.	16 bytes

No.	Item	Description	Length
6	pid	In the integrated trace log, this item indicates the process ID assigned by the OS. In log entries output by JP1/AO-specific products, pid indicates the hash value assigned by the JavaVM to the Runtime instance.	8 bytes
7	tid	In the integrated trace log, this item contains a value derived from the thread name. In log entries output by JP1/AO-specific products, tid indicates the hash value assigned by the JavaVM to the Thread instance.	8 bytes
8	ID	A message ID including a prefix that identifies the product.	16 bytes
9	Event type	The type of event for which the log entry was output.	4 bytes
10	Message text	The text of the message.	4,095 bytes or less
11	Linefeed code	CRLF:0x0D, 0x0A	4 bytes

13.9.2 Collecting log information

The following describes how to acquire log information.

Preparation

- Log in to the JP1/AO server as a user with Administrators permission for the OS.

Procedure

1. Execute the `hcmdsgetlogs` command.

Log information is output to a file with the following name in the output folder you specify.

- `Automation_1st_log.jar`

Important note

The following files are also output when you execute the command. Hitachi does not disclose the contents or format of these files.

- `output-folder\Automation_log.jar`
- `output-folder\AJS_log.jar`
- `output-folder\HiCommand_log.jar`
- `output-folder\HiCommand_log.hdb.jar`
- `output-folder\HiCommand_log.db.jar`
- `output-folder\HiCommand_log.csv.jar`

In a cluster environment, acquire log information on the primary and secondary servers.

13.9.3 Task log details

JP1/AO outputs information about tasks starting and stopping, called plug-ins, and other activity to the task log.

When you execute a task, JP1/AO creates a folder to which the log information for that task is output. You can see or download the task log file in the **Tasks** view, **Task Details** dialog box, and **Debug-Tasks** view.

You can specify the maximum task log size value (KB) of the task log file size section of the property file (config_user.properties). If the task log file size exceeds the maximum value, task log data is overwritten from the oldest.

(1) Name and location of task log files

The name and location of the task log file are as follows:

- *JP1/AO-installation-folder\data\task\task-ID\task_task-ID_1.log*
In a cluster environment, replace *JP1/AO-installation-foder* with *shared-folder-name\jp1ao*.

(2) Information output to task log

The following shows the information output to the task log, and shows an example of a task log entry.

Table 13–4: Contents of task log

Output sequence	Type	Example message
1	Basic information	<i>message-ID</i> Plug-in execution has started.
2	Plug-in definition	<i>message-ID</i> Plug-in definition information
3	Property (before plug-in execution)	<i>message-ID</i> Property information at plug-in execution
4	Basic information	<i>message-ID</i> Plug-in execution has completed.
5	Property (after plug-in execution)	<i>message-ID</i> Property information after plug-in execution
6	Standard output	Standard output of plug-in execution results
--	Error information	<i>message-ID</i> An error occurred during plug-in execution.
--	Debug information	<i>message-ID</i> Arbitrary debug information
--	Messages related to task operation	<ul style="list-style-type: none">• <i>message-ID</i> Task execution has stopped.• <i>message-ID</i> The task was forcibly stopped.• <i>message-ID</i> The failed step was retried.• <i>message-ID</i> The step after the failed one was retried.
--	Messages related to debug operation	<ul style="list-style-type: none">• <i>message-ID</i> Processing stopped before (or after) execution of plug-in processing.• <i>message-ID</i> Plug-in processing resumed.• <i>message-ID</i> Changes in plug-in property values were applied.• <i>message-ID</i> Changes in plug-in return values were applied.

Legend:

--: Output when a failure occurred, or task or debug operation was performed.

The following is an example of the information output to the task log:

```
KNAE08001-I Plug-in execution started (Task name: JP1/AJS root jobnet
transition_multi_20131107141827, Task ID: 5859, Step ID: /
```

```

getRootJobnetKeyList, Execution ID: @A571).
KNAE08005-I vendor=com.hitachi.software.dna.cts.jp1
KNAE08005-I name=osReadCSVExcelFileColumn
KNAE08005-I version=01.10.00
:
KNAE08006-I property=plugin.destinationHost, value=192.168.1.1
KNAE08111-I Remote command execution started.
KNAE08102-I Remote command execution succeeded (Command:
osReadCSVExcelFileColumn.bat "C:\AJS.xlsx" "sheet 1" "1" "" "" "" "" 2>&1).
:
KNAE08010-I <Standard output (first line)>
KNAE08010-I <Standard output (second line)>
:
KNAE08010-I Standard output (nth line)>
KNAE08002-I Plug-in execution finished (Task name: Obtain JP1/Cm2 monitored
node list, Task ID: 3969, Step ID: /getNodeListFileJP1Cm2, Execution ID:
@A105, Plug-in return value: 0).

```

(3) Output levels for the task log

You can set the output level for the task log in a shared service property.

The output level setting determines the information output to the task log. The following table describes the information output to the task log at each output level.

Table 13–5: Task log output level

Output level	Output information								Task related	Debugger function	Description
	Error information	Basic information	Plug-in definition (before plug-in execution)	Property (before plug-in execution)	Plug-in definition (after plug-in execution)	Property (after plug-in execution)	Standard output	Debug information			
0	Y	N	N	N	N	N	N	N	N	N	Only error information is output.
10	Y	Y	N	N	Y/N	Y/N	Y/N	N	Y	Y	When the return value of the plug-in is 0, JP1/AO outputs error information and basic information. When the return value of the plug-in is other than 0, JP1/AO outputs error information, basic information, plug-in definitions (after plug-in execution), properties (after plug-in execution), and standard output.
20	Y	Y	Y	N	N	Y	Y/N	N	Y	Y	When the return value of the plug-in is 0, JP1/AO outputs error information, basic information, plug-in definitions (before plug-in execution), and properties (after plug-in execution).

Output level	Output information								Task related	Debugger function	Description
	Error information	Basic information	Plug-in definition (before plug-in execution)	Property (before plug-in execution)	Plug-in definition (after plug-in execution)	Property (after plug-in execution)	Standard output	Debug information			
20	Y	Y	Y	N	N	Y	Y/N	N	Y	Y	When the return value of the plug-in is other than 0, JP1/AO outputs error information, basic information, plug-in definitions (before plug-in execution), properties (after plug-in execution), and standard output.
30	Y	Y	Y	Y #	N	Y #	Y	N	Y	Y	JP1/ AO outputs information other than plug-in definitions (after plug-in execution) and debug information.
40	Y	Y	Y	Y #	N	Y #	Y	Y	Y	Y	JP1/ AO outputs all information other than plug-in definitions (after plug-in execution) for debugging purposes.

Legend:

Y: Output according to the log level of the message when an occurrence subject to message output occurs.

N: Not output.

Y/N: Output when the plug-in return value is a value other than 0.

#

When the data type of the property is *password*, ******* is output as the property value.

Related topics

- [7.1 Procedure for setting service share properties](#)

(4) Plug-in return values output to task log files

Return values of plug-ins are output to task log files, but return values of the flow plug-in, interval plug-in, judge returncode plug-in, abnormal-end plug-in, and judge value plug-in are not output to task log files.

When a task is forcibly stopped, or a failure occurs, the return value of the plug-in to be output to the task log and the return value of the step displayed in the **Task Details** dialog box might be different. If this happens, take action according to the description for the return values of steps displayed in the **Task Details** dialog box.

Note that the judgment of the subsequent-step execution condition is performed according to the return values of steps.

Related topics

- Overview of subsequent step conditions in the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*

13.9.4 Integrated trace log and event log details

(1) Name and location of integrated trace log

The name and location of the integrated trace log files are as follows:

- `system-drive\Program Files (x86)\Hitachi\HNTRLib2\spool\hntr2[n].log`
[n] is an integer from 1 to 4.

You can view the contents of the event log in the Windows Event Viewer.

(2) Output levels for integrated trace log and event log

You can set the output level of the integrated trace log and event log in the properties file (`config_user.properties`). The following table describes the information output to the integrated trace log and event log at each output level.

Table 13–6: Integrated trace log and event log output levels

Output level	Output information
0	<ul style="list-style-type: none">• Severe error, server fails to start• A server starts or stops
10	<ul style="list-style-type: none">• A command starts or finishes
20	<ul style="list-style-type: none">• Inter-process communication occurs

Related topics

- *Properties file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

13.9.5 Public log details

(1) Name and location of public log file

The name and location of public log files are as follows. Note that the public log files are output in WRAP2 format.

- Location
`JPI/AO-installation-folder\logs`
- File name
`Server[n].log`
`Command_command-name[n].log`
[n] is an integer. In a cluster environment, replace `JPI/AO-installation-folder` with `shared-folder-name\jplao`.

(2) Output levels for public logs

The following table describes the information output to the public log at each output level.

Table 13–7: Public log output levels

Output level	Output information
0	<ul style="list-style-type: none">• Severe error, server fails to start• A server starts or stops
10	<ul style="list-style-type: none">• A command starts or finishes
20	<ul style="list-style-type: none">• Inter-process communication occurs



Appendix

A. Reference Information

These appendixes provide reference information for users of JP1/AO.

A.1 List of JP1 events output by JP1/AO

(1) List of JP1 events

The following table lists the JP1 events output by JP1/AO.

Table A–1: JP1 events

Event ID	Event name	Generated when	Message ID
0x00007000	Task status detection event (Waiting for Response) ^{#1#2}	A task enters Waiting for Response status	KNAE01317-I
	Task status detection event (Completed) ^{#1}	A task enters Completed status	KNAE01315-I
	Task status detection event (Failed) ^{#1}	A task enters Failed status	KNAE01318-E
	Task status detection event (Canceled) ^{#1}	A task enters Canceled status	KNAE01322-I
0x00007010	JP1/AO start event	The JP1/AO service starts	KNAE03020-I
	JP1/AO stop event	The JP1/AO service stops	KNAE03021-I
0x00007020	Abnormal detection event for task processing engine	An error is detected in the task processing engine	KNAE01323-E
0x00007030	Database abnormal detection event	A database error is detected	KNAE01321-E

#1

JP1/AO monitors the status of tasks at regular intervals (once every 30 seconds by default). The event is generated when JP1/AO detects the change, not when the change itself occurs.

#2

If a task transitions to Waiting for Response status and the user enters a response in the **Respond** dialog box within 30 seconds of the transition, the JP1 event might not be issued because the task has already transitioned to another status.

(2) JP1 event attributes

The following table lists the attributes of the JP1 events output by JP1/AO.

Table A–2: Attributes of task status detection event (Waiting for Response)

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007000
	Message	MESSAGE	KNAE01317
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	<i>user-who-submitted-service-for-execution</i>

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	/HITACHI/JP1/AO/TASK
	Object name	OBJECT_NAME	<i>task-name</i>
	Root object type	ROOT_OBJECT_TYPE	/HITACHI/JP1/AO/SERVICE
	Root object name	ROOT_OBJECT_NAME	<i>service-name</i>
	Object ID	OBJECT_ID	<i>task-ID</i>
	Occurrence	OCCURRENCE	WAITING_RESPONSE
	Start date	START_DATE	<i>date-and-time-when-task-starts</i>
	End date	END_DATE	<i>date-and-time-when-task-ends</i>
Extended attributes (fixed information)	Resource group name	RESOURCE_GROUP	<i>resource-group-name</i>
	Task type	TASK_KIND	<i>task-type</i>
	Service category	SERVICE_CATEGORY	<i>service-category</i>
	Task status	TASK_STATUS	<i>task-status</i>
	Scheduled submission date	PLANNED_START_DATE	<i>scheduled-submission-date</i> ^{#1}
	Date and time task submitted	EXECUTION_DATE	<i>date-and-time-task-submitted</i>
	Recurrence pattern	SCHEDULE_PERIOD	<i>recurrence-pattern</i> ^{#2}
	Recurrence time	SCHEDULE_TIME	<i>recurrence-time</i> ^{#2}
	Recurrence start date	SCHEDULE_START_DATE	<i>recurrence-start-date</i> ^{#2}
	URL of the information for the applicable task	TASK_DETAILS_URL	<i>URL-of-information-for-applicable-task</i>

#1

Output for recurring tasks or tasks submitted on scheduled dates.

#2

Output for recurring tasks.

Table A–3: Attributes of task status detection event (Completed)

Attribute type	Item	Attribute name	Content
Basic attribute	Event ID	ID	0x00007000
	Message	MESSAGE	KNAE01315
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	<i>user-who-submitted-service-for-execution</i>
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	/HITACHI/JP1/AO/TASK

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Object name	OBJECT_NAME	<i>task-name</i>
	Root object type	ROOT_OBJECT_TYPE	/HITACHI/JP1/AO/SERVICE
	Root object name	ROOT_OBJECT_NAME	<i>service-name</i>
	Object ID	OBJECT_ID	<i>task-ID</i>
	Occurrence	OCCURRENCE	END
	Start date	START_DATE	<i>date-and-time-when-task-starts</i>
	End date	END_DATE	<i>date-and-time-when-task-ends</i>
Extended attributes (fixed information)	Resource group name	RESOURCE_GROUP	<i>resource-group-name</i>
	Task type	TASK_KIND	<i>task-type</i>
	Service category	SERVICE_CATEGORY	<i>service-category</i>
	Task status	TASK_STATUS	<i>task-status</i>
	Scheduled submission date	PLANNED_START_DATE	<i>scheduled-submission-date</i> ^{#1}
	Date and time task submitted	EXECUTION_DATE	<i>date-and-time-task-submitted</i>
	Recurrence pattern	SCHEDULE_PERIOD	<i>recurrence-pattern</i> ^{#2}
	Recurrence time	SCHEDULE_TIME	<i>recurrence-time</i> ^{#2}
	Recurrence start date	SCHEDULE_START_DATE	<i>recurrence-start-date</i> ^{#2}
URL of the information for the applicable task	TASK_DETAILS_URL	<i>URL-of-information-for-applicable-task</i>	

#1

Output for recurring tasks or tasks submitted on scheduled dates.

#2

Output for recurring tasks.

Table A-4: Attributes of task status detection event (Failed)

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007000
	Message	MESSAGE	KNAE01318
Extended attributes (common information)	Severity	SEVERITY	Error
	User name	USER_NAME	<i>user-who-submitted-service-for-execution</i>
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	/HITACHI/JP1/AO/TASK
	Object name	OBJECT_NAME	<i>task-name</i>

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Root object type	ROOT_OBJECT_TYPE	/HITACHI/JP1/AO/SERVICE
	Root object name	ROOT_OBJECT_NAME	<i>service-name</i>
	Object ID	OBJECT_ID	<i>task-ID</i>
	Occurrence	OCCURRENCE	STOP
	Start date	START_DATE	<i>date-and-time-when-task-starts</i>
	End date	END_DATE	<i>date-and-time-when-task-ends</i>
Extended attributes (fixed information)	Resource group name	RESOURCE_GROUP	<i>resource-group-name</i>
	Task type	TASK_KIND	<i>task-type</i>
	Service category	SERVICE_CATEGORY	<i>service-category</i>
	Task status	TASK_STATUS	<i>task-status</i>
	Scheduled submission date	PLANNED_START_DATE	<i>scheduled-submission-date</i> ^{#1}
	Date and time task submitted	EXECUTION_DATE	<i>date-and-time-task-submitted</i>
	Recurrence pattern	SCHEDULE_PERIOD	<i>recurrence-pattern</i> ^{#2}
	Recurrence time	SCHEDULE_TIME	<i>recurrence-time</i> ^{#2}
	Recurrence start date	SCHEDULE_START_DATE	<i>recurrence-start-date</i> ^{#2}
URL of the information for the applicable task	TASK_DETAILS_URL	<i>URL-of-information-for-applicable-task</i>	

#1

Output for recurring tasks or tasks submitted on scheduled dates.

#2

Output for recurring tasks.

Table A–5: Attributes of task status detection event (Canceled)

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007000
	Message	MESSAGE	KNAE01322
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	<i>user-who-submitted-service-for-execution</i>
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	/HITACHI/JP1/AO/TASK
	Object name	OBJECT_NAME	<i>task-name</i>
	Root object type	ROOT_OBJECT_TYPE	/HITACHI/JP1/AO/SERVICE

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Root object name	ROOT_OBJECT_NAME	<i>service-name</i>
	Object ID	OBJECT_ID	<i>task-ID</i>
	Occurrence	OCCURRENCE	NORESTART
	Start date	START_DATE	<i>date-and-time-when-task-starts</i>
	End date	END_DATE	<i>date-and-time-when-task-ends</i>
Extended attributes (fixed information)	Resource group name	RESOURCE_GROUP	<i>resource-group-name</i>
	Task type	TASK_KIND	<i>task-type</i>
	Service category	SERVICE_CATEGORY	<i>service-category</i>
	Task status	TASK_STATUS	<i>task-status</i>
	Scheduled submission date	PLANNED_START_DATE	<i>scheduled-submission-date</i> ^{#1}
	Date and time task submitted	EXECUTION_DATE	<i>date-and-time-task-submitted</i>
	Recurrence pattern	SCHEDULE_PERIOD	<i>recurrence-pattern</i> ^{#2}
	Recurrence time	SCHEDULE_TIME	<i>recurrence-time</i> ^{#2}
	Recurrence start date	SCHEDULE_START_DATE	<i>recurrence-start-date</i> ^{#2}
	URL of the information for the applicable task	TASK_DETAILS_URL	<i>URL-of-information-for-applicable-task</i>

#1

Output for recurring tasks or tasks submitted on scheduled dates.

#2

Output for recurring tasks.

Table A–6: Attributes of JP1/AO start event

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007010
	Message	MESSAGE	KNAE03020
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	System
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	--
	Object name	OBJECT_NAME	SYSTEM
	Root object type	ROOT_OBJECT_TYPE	--
	Root object name	ROOT_OBJECT_NAME	SYSTEM

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Object ID	OBJECT_ID	--
	Occurrence	OCCURRENCE	START
	Start date	START_DATE	<i>date-and-time-when-JP1/AO-starts</i>
	End date	END_DATE	--

Legend

--: Not used.

Table A–7: Attributes of JP1/AO stop event

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007010
	Message	MESSAGE	KNAE03021
Extended attributes (common information)	Severity	SEVERITY	Information
	User name	USER_NAME	System
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	--
	Object name	OBJECT_NAME	SYSTEM
	Root object type	ROOT_OBJECT_TYPE	--
	Root object name	ROOT_OBJECT_NAME	SYSTEM
	Object ID	OBJECT_ID	--
	Occurrence	OCCURRENCE	STOP
	Start date	START_DATE	--
End date	END_DATE	<i>date-and-time-when-JP1/AO-stops</i>	

Legend

--: Not used.

Table A–8: Attributes of abnormal detection event for the task processing engine

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007020
	Message	MESSAGE	KNAE01323
Extended attributes (common information)	Severity	SEVERITY	Error
	User name	USER_NAME	System
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	--
	Object name	OBJECT_NAME	SYSTEM

Attribute type	Item	Attribute name	Content
Extended attributes (common information)	Root object type	ROOT_OBJECT_TYPE	--
	Root object name	ROOT_OBJECT_NAME	SYSTEM
	Object ID	OBJECT_ID	--
	Occurrence	OCCURRENCE	EXCEPTION
	Start date	START_DATE	--
	End date	END_DATE	--

Legend

--: Not used.

Table A–9: Attributes of database abnormal detection event

Attribute type	Item	Attribute name	Content
Basic attributes	Event ID	ID	0x00007030
	Message	MESSAGE	KNAE01321
Extended attributes (common information)	Severity	SEVERITY	Error
	User name	USER_NAME	System
	Product name	PRODUCT_NAME	/HITACHI/JP1/AO
	Object type	OBJECT_TYPE	--
	Object name	OBJECT_NAME	SYSTEM
	Root object type	ROOT_OBJECT_TYPE	--
	Root object name	ROOT_OBJECT_NAME	SYSTEM
	Object ID	OBJECT_ID	--
	Occurrence	OCCURRENCE	EXCEPTION
	Start date	START_DATE	--
End date	END_DATE	--	

Legend

--: Not used.

A.2 Outputting audit log entries

An audit log is a file containing information about the operations performed in a JP1/AO system. An audit log entry includes information about who executed what operation, at what time.

(1) Event types output to audit log

The event type is an identifier that categorizes the events output to the audit log. The following table lists the types of event output to the audit log, and when JP1/AO outputs each type of event.

Table A–10: Event types output to audit log

No.	Event type	Event name	Description	When output by JP1/AO	Output message
1	StartStop	Startup or shutdown	JP1/AO has started successfully or has failed to start.	A user successfully executes the <code>hcmdssrv /start</code> command	KNAE23001-I
				A user attempts to execute the <code>hcmdssrv /start</code> command, but the attempt fails	KNAE23017-E
			JP1/AO has stopped.	A user successfully executes the <code>hcmdssrv /stop</code> command	KNAE23002-I
2	Authentication	Identification and authentication	User authentication has failed.	User authentication fails at login	KNAE20001-E
			A user has logged in successfully, login has failed, or a user has logged out.	A user logs in successfully	KNAE20002-I
				A user attempts to log in, but the attempt fails	KNAE20003-W
				A user logs out successfully	KNAE20004-I
3	ConfigurationAccess	Configuration definition	A user group has been configured successfully, or an attempt to configure a user group has failed.	A user successfully creates a user group	KNAE20006-I
				A user attempts to create a user group, but the attempt fails	KNAE20007-E
				A user successfully edits a user group	KNAE20008-I
				A user attempts to edit a user group, but the attempt fails	KNAE20009-E
				A user successfully deletes a user group	KNAE20010-I
				A user attempts to delete a user group, but the attempt fails	KNAE20011-E
			An attempt to assign a user group was successful or failed.	A user successfully assigns a user group	KNAE20044-I
				A user attempts to assign a user group, but the attempt fails	KNAE20045-E
			An attempt to define a connection destination was successful or failed.	A user successfully creates a connection destination	KNAE20012-I
				A user attempts to create a connection destination, but the attempt fails	KNAE20013-E
				A user successfully edits a connection destination	KNAE20014-I
				A user attempts to edit a connection destination, but the attempt fails	KNAE20015-E
				A user successfully deletes a connection destination	KNAE20016-I

No.	Event type	Event name	Description	When output by JP1/AO	Output message
3	Configurati onAccess	Configurat ion definition	An attempt to define a connection destination was successful or failed.	A user attempts to delete a connection destination, but the attempt fails	KNAE20017-E
			An attempt to set a shared service property was successful or failed.	A user successfully edits a shared service property	KNAE21005-I
				A user attempted to edit a shared service property, but the attempt fails	KNAE21006-E
			An attempt to configure a resource group was successful or failed.	A user successfully creates a resource group	KNAE20020-I
				A user attempts to create a resource group, but the attempt fails	KNAE20021-E
				A user successfully edits a resource group	KNAE20022-I
				A user attempts to edit a resource group, but the attempt fails	KNAE20023-E
				A user successfully deletes a resource group	KNAE20024-I
				A user attempts to delete a resource group, but the attempt fails	KNAE20025-E
			An attempt to execute a command was successful or failed.	A user successfully executes a command (backupsystem/ restoresystem/ setupcluster/ encryptpassword)	KNAE23003-I
				A user attempts to execute a command (backupsystem/ restoresystem/ setupcluster/ encryptpassword), but the attempt fails	KNAE23004-E
			An attempt to develop a service template was successful or failed.	A user successfully creates a service template	KNAE20048-I
				A user attempts to create a service template, but the attempt fails	KNAE20049-E
				A user successfully edits a service template	KNAE20050-I
				A user attempts to edit a service template, but the attempt fails	KNAE20051-E
				A user successfully deletes a service template	KNAE20052-I
				A user attempts to delete a service template, but the attempt fails	KNAE20053-E
				A user successfully duplicates a service template	KNAE20054-I

No.	Event type	Event name	Description	When output by JP1/AO	Output message
3	Configurati onAccess	Configurat ion definition	An attempt to develop a service template was successful or failed.	A user attempts to duplicate a service template, but the attempt fails	KNAE20055-E
				A user successfully builds a service template	KNAE20056-I
				A user attempts to build a service template, but the attempt fails	KNAE20057-E
				A user successfully releases a service template	KNAE20058-I
				A user attempts to release a service template, but the attempt fails	KNAE20059-E
				A user successfully creates a plug-in	KNAE20060-I
				A user attempts to create a plug-in, but the attempt fails	KNAE20061-E
				A user successfully edits a plug-in	KNAE20062-I
				A user attempts to edit a plug-in, but the attempt fails	KNAE20063-E
				A user successfully duplicates a plug-in	KNAE20064-I
				A user attempts to duplicate a plug-in, but the attempt fails	KNAE20065-E
				A user successfully deletes a plug-in	KNAE20066-I
				A user attempts to delete a plug-in, but the attempt fails	KNAE20067-E
4	ContentAcc ess	Access to critical informatio n	An attempt to add, edit, delete, or submit a service was successful or failed.	A user successfully adds a service	KNAE20026-I
				A user attempts to add a service, but the attempt fails	KNAE20027-E
				A user successfully edits a service	KNAE20028-I
				A user attempts to edit a service, but the attempt fails	KNAE20029-E
				A user successfully deletes a service	KNAE20030-I
				A user attempts to delete a service, but the attempt fails	KNAE20031-E
				A user successfully submits a service	KNAE20032-I
				A user attempts to submit a service, but the attempt fails	KNAE20033-E
			An attempt to suspend, resume, or cancel a task schedule was successful or failed.	A user successfully suspends a task schedule	KNAE20034-I
A user attempts to suspend a task schedule, but the attempt fails	KNAE20035-E				

No.	Event type	Event name	Description	When output by JP1/AO	Output message
4	ContentAccess	Access to critical information	An attempt to suspend, resume, or cancel a task schedule was successful or failed.	A user successfully resumes a task schedule	KNAE20036-I
				A user attempts to resume a task schedule, but the attempt fails	KNAE20037-E
				A user successfully cancels a task schedule	KNAE20038-I
				A user attempts to cancel a task schedule, but the attempt fails	KNAE20039-E
			An attempt to stop a task was successful or failed.	A user successfully stops execution of a task	KNAE20040-I
				A user attempts to stop execution of a task, but the attempt fails	KNAE20041-E
			An attempt to forcibly stop a task was successful or failed.	A user successfully performs forced stop of a task	KNAE20068-I
				A user attempts to forcibly stop a task, but the attempt fails	KNAE20069-E
			An attempt to retry a task was successful or failed.	A user successfully retries the failed step of a task	KNAE20070-I
				A user attempts to retry the failed step of a task, but the attempt fails	KNAE20071-E
				A user successfully retries the step after the failed one of a task	KNAE20072-I
				A user attempts to retry the step after the failed one of a task, but the attempt fails	KNAE20073-E
			An attempt to archive tasks, delete task histories, and delete debug tasks were successful or failed.	A user successfully archives tasks	KNAE20042-I
				A user attempts to archive tasks, but the attempt fails	KNAE20046-E
				A user successfully deletes task histories	KNAE20043-I
				A user attempts to delete task histories, but the attempt fails	KNAE20047-E
				A user successfully deletes a debug task	KNAE20076-I
				A user attempts to delete a debug task, but the attempt fails	KNAE20077-E
				A user successfully archives tasks automatically	KNAE21001-I
				A user attempts to archive tasks automatically, but the attempt fails	KNAE21003-E
A user successfully deletes task histories automatically	KNAE21002-I				
A user attempts to delete task histories automatically, but the attempt fails	KNAE21004-E				

No.	Event type	Event name	Description	When output by JP1/AO	Output message
4	ContentAccess	Access to critical information	An attempt to archive tasks, delete task histories, and delete debug tasks were successful or failed.	A user successfully deletes a debug task automatically	KNAE21007-I
				A user attempts to delete a debug task automatically, but the attempt fails	KNAE21008-E
			An attempt to debug a service template was successful or failed.	A user successfully debugs a service template	KNAE20074-I
				A user attempts to debug a service template, but the attempt fails	KNAE20075-E
			An attempt to execute a command was successful or failed.	A user successfully executes the <code>submittask</code> command	KNAE23005-I
				A user attempts to execute the <code>submittask</code> command, but the attempt fails	KNAE23006-E
				A user successfully executes the <code>stoptask</code> command	KNAE23007-I
				A user attempts to execute the <code>stoptask</code> command, but the attempt fails	KNAE23008-E
				A user successfully executes the <code>listtasks</code> command	KNAE23009-I
				A user attempts to execute the <code>listtasks</code> command, but the attempt fails	KNAE23010-E
				A user successfully executes the <code>listservices</code> command	KNAE23011-I
				A user attempts to execute the <code>listservices</code> command, but the attempt fails	KNAE23012-E
				A user successfully executes the <code>importservicetemplate</code> command	KNAE23013-I
				A user attempts to execute the <code>importservicetemplate</code> command, but the attempt fails	KNAE23014-E
A user successfully executes the <code>deleteservicetemplate</code> command	KNAE23015-I				
A user attempts to execute the <code>deleteservicetemplate</code> command, but the attempt fails	KNAE23016-E				

(2) Storage format of audit log output

The following table shows the names of the files to which JP1/AO outputs audit log entries.

Table A–11: Output destination for audit logs

Environment	Output destination	Output file name
Non-cluster environment	<i>JP1/AO-installation-folder</i> \logs ^{#1}	Audit <i>n</i> .log ^{#2}
Cluster environment	<i>shared-folder</i> \jp1ao\logs	

#1

You can change the output destination for audit logs. To change the output destination, alter the setting in a property file.

#2

n is replaced with the number of the log file.

Related topics

- *Properties file (config_user.properties)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

(3) Output format of audit log entries

This section describes the files to which JP1/AO outputs audit log entries, and the contents of these audit log entries.

(a) Audit log output format

An audit log entry consists of the string CALFHM indicating the information is formatted as an audit log, followed by the revision number of the audit log, and finally the relevant output items.

The following figure shows the format in which audit log entries are output:

Figure A–1: Audit log output format

```
CALFHM 1.0.output-item-1=value-1.output-item-2=value-2....output-item-n=value-n
```

(b) Output destination of audit log entries

For details about the output destination for audit logs, see [A.2\(2\) Storage format of audit log output](#).

(c) Output items

There are three types of information output to the audit log:

- Header information
The date and time when the log entry was output, and other information derived from the OS.
- Common information
Information used to categorize and monitor the event that triggered the audit log entry.
- Event-specific information
Detailed information about the event that triggered the audit log entry.

The following table lists the items output to the audit log:

Table A–12: Audit log output items

No.	Output item			Value	
	Type	Name	Output attribute name		
1	Header information	Common specification identifier	--	CALFHM	
2		Common specification revision number	--	1.0	
3	Common information	Sequence number	seqnum	<i>sequence-number</i>	
4		Message ID	msgid	<i>message-ID</i>	
5		Date and time	date	<i>date-and-time</i>	
6		Source program name	progid	JP1AO	
7		Source component	compid	<ul style="list-style-type: none"> • Command • GUI • Server 	
8		Source process ID	pid	<i>process-ID</i>	
9		Location information	ocp:host/ipv4/ipv6	<i>host-name</i>	
			outp:host/ipv4/ipv6	<i>host-name</i>	
			subjp:host/ipv4/ipv6	<i>host-name</i>	
			dtp:host/ipv4/ipv6	<i>host-name</i>	
	agent:host/ipv4/ipv6		<i>host-name</i>		
10	Event type	ctgry	<ul style="list-style-type: none"> • Authentication • ConfigurationAccess • ContentAccess • ExternalService • StartStop 		
11			Event result	result	<ul style="list-style-type: none"> • Success • Failure
12			Subject identification information	subj:uid	<i>login-user-ID</i>
	subj:euid	<i>Windows-user-ID</i>			
	subj:pid	<i>process-ID</i>			
13	Event-specific information	Object information	obj	<ul style="list-style-type: none"> • autoAuth • autoJOB 	
14		Operation information	op	<ul style="list-style-type: none"> • Add • Delete • Login • Logout • Start • Stop • Update 	
15		Log type information	logtype	BasicLog	

No.	Output item			Value
	Type	Name	Output attribute name	
16	Event-specific information	Optional message	msg	<i>message</i>

Legend

--: Not output.

(d) Example of audit log output

The following is an example of the information output in an audit log entry.

```
CALFHM 1.0, seqnum=1, msgid=KNAE23001-I, date=2012-01-01T00:00:00.000+09:00,
progid=JP1AO, compid=Command, pid=1234, ocp:host=host01, ctgry=StartStop,
result=Success, subj:euid=user01, obj=autoJOB, op=Start, logtype=BasicLog,
msg="A service has started"
```

(4) Configuring JP1/AO to output audit logs

You can configure JP1/AO to output audit logs by a setting in a property file (config_user.properties). For details on the property file (config_user.properties), see the *Job Management Partner 1/Automatic Operation Configuration Guide*.

Related topics

- *Properties file (config_user.properties) in the Job Management Partner 1/Automatic Operation Configuration Guide*

A.3 JP1/AO services

When you install JP1/AO, the following JP1/AO services are registered in the operating system.

Table A–13: JP1/AO services

Service display name	Service name	Startup type	Product
HAutomation Engine Web Service	AutomationWebService	Automatic [#]	JP1/AO
HiRDB/EmbeddedEdition_HD0	HiRDBEmbeddedEdition_HD0	Automatic	Common Component
HBase Storage Mgmt Common Service	HBaseStgMgmtComService	Automatic [#]	Common Component
HBase Storage Mgmt Web Service	HBaseStgMgmtWebService	Automatic [#]	Common Component
HBase Storage Mgmt Web SSO Service	HBaseStorageMgmtWebSSOService	Manual	Common Component
HAutomation Engine	JP1_AJS2	Manual	JP1/AO
HAutomation Engine Database_JF0	HiRDBEmbeddedEdition_JF0	Manual	JP1/AO

#

Changes to Manual after a cluster environment is set up.

For details on the JP1/Base services of prerequisite products, see the JP1/Base documentation.

Related topics

- *Starting and stopping JP1/Base* in the *Job Management Partner 1/Base User's Guide*

A.4 Version changes

(1) Changes in version 10-10

- A description about how to set preset properties was added.
- A description about linkage with JP1/AJS3 was added.
- A description about linkage with JP1/IM - NP business content was added.
- A description about the storage locations of service templates for the JP1/AO standard package and JP1/AO content set was added.
- The Develop role, which is a role that can be set for resource groups, was added.
- DevelopGroup was added to the built-in user group.
- Telnet was added as a protocol that can be used.
- Service templates can now be developed with the Admin role.
- A description about maintenance was added.
- In the **Submit Service** dialog box, functionality for specifying the name and description of a task and the property values for a direct-access URL was added.
- Information about estimating query parameters was added.
- A procedure for developing service templates was added.
- The Develop role was added to the *Who can perform this task* section.
- Restrictions applying to the specification of categories were added.

Index

A

- access control
 - using user group and resource group 65
- access control using
 - connection destinations 70
- Active Directory
 - linking with 83
- Active Directory linking with JP1/AO
 - registering group 159
- adding
 - preset properties 22
 - service 25, 106
- AdminGroup 67
- Admin role 68
- allocating resource groups
 - user groups 64
- allocating roles
 - user groups 64
- assigning
 - categories 59
- audit log
 - event types 216
 - output format 221
 - outputting 215
 - storage format 220
- audit logs
 - enabling output 223
- authentication
 - linking with JP1/Base 82
- authentication-information management 71

B

- backup and restoration
 - note 79
- basic task
 - post-review preparation phase 19
 - review phase 19
- basic tasks
 - day-to-day operation 18
 - maintenance phase 18
 - preparation phase 16
- built-in resource groups 67
- built-in user groups 67

C

- categories
 - assigning 59
- changing
 - password (another user) 145
 - password (one's own) 146
 - passwords 61
 - User Management permission 147
- changing affiliation
 - user groups 64
- collecting
 - log information 202
- configuring
 - Link&Launch 94
- connection destination
 - defining 164
 - deleting 166
 - editing definition information 165
 - managing 70
- connection destination definitions
 - creating 70
 - deleting 70
 - editing 70
- connection destinations
 - access control using 70
 - defaults 78
 - definition parameters 73
 - enabling management 73
 - managing 163
- connection-restriction 70
- creating
 - connection destination definitions 70
 - resource group 153
 - resource groups 64
 - service template 22
 - user group 157
 - user groups 64

D

- database
 - maintenance (cluster configuration) 181
 - maintenance (non-cluster configuration) 179
- daylight saving
 - time zones 32

- day-to-day operation
 - basic tasks 18
- default user
 - JP1/AO 62
- defining
 - connection destination 164
- defining service
 - intervening action 26
- definition parameters
 - connection destinations 73
- deleting
 - connection destination 166
 - connection destination definitions 70
 - resource group 155
 - resource groups 64
 - service 25, 109
 - service templates 22
 - task history 135
 - user group 162
 - user groups 64
 - users 61
- deleting from JP1/AO
 - user 151
- detailed task information
 - outputting in a batch 137
- DevelopGroup 67
- Develop role 68
- direct-access URL 90
 - format 90
 - parameters 90
- display format
 - task summary 46

E

- editing
 - connection destination definition information 165
 - connection destination definitions 70
 - resource group 154
 - resource groups 64
 - service 25, 108
 - user group 158
 - user groups 64
- email notification 88
 - settings 88
- enabling management
 - connection destinations 73
- entry format

- connection destination 77
- event log
 - detail 206
- events
 - list of JP1 events 209
- executing
 - services 111

F

- features
 - list of JP1/AO features 20
- format
 - preset property definition file 57

G

- groups
 - managing 64

H

- history
 - deleting 35

I

- immediate
 - service execution timing 48
 - task categories 47
- integrated trace log
 - detail 206
- intervening action
 - defining service 26
 - submitting service 27
- IP addresses
 - resolving host names 75

J

- JP1/AO
 - default user 62
 - logging in 96, 97
 - using 15
- JP1/AO
 - operation overview 16
- JP1/AO Content Set
 - storage location 23
- JP1/AO server
 - restoring remotely using backup file 188

- JP1/AO service
 - note on restarting 80
- JP1/AO standard-package plug-in
 - storage location 23
- JP1/AO system
 - starting (cluster configuration) 185
 - starting (non-cluster configuration) 184
 - stopping (cluster configuration) 187
 - stopping (non-cluster configuration) 186
- JP1/IM event monitoring
 - linking 85
- JP1/IM - NP business content
 - linking with 95
- JP1 event
 - list 209
 - output by JP1/AO 209
- JP1 event linkage 85
- JP1 events
 - attributes 209

L

- Link&Launch
 - configuring 94
- linking
 - JP1/IM event monitoring 85
- linking with JP1/Base
 - authentication 82
- linking with JP1/IM - NP business content 95
- list of services
 - exporting 110
 - outputting 110
- locking
 - user 148
- log information
 - collecting 202
 - detailed description 201
 - event log 201
 - format 201
 - integrated trace log 201
 - public logs 201
 - task logs 201

M

- maintenance 167
 - backing up (cluster environment) 170
 - backing up (non-cluster environment) 168

- data that is restored 80
- JP1/AO 79
- restoring (cluster environment) 175
- restoring backup (non-cluster environment) 173
- starting JP1/AO system (cluster configuration) 185
- starting JP1/AO system (non-cluster configuration) 184
- stopping JP1/AO system (cluster configuration) 187
- stopping JP1/AO system (non-cluster configuration) 186
- maintenance phase
 - basic tasks 18
- managing
 - connection destination 70
 - connection destinations 163
 - groups 64
 - service 25
 - services 105
 - service templates 22, 99
 - tasks 33, 116
 - users 61, 141
- managing progress
 - task 38
- ModifyGroup 67
- Modify role 68
- monitoring-startup linkage 85

O

- outputting
 - audit log 215

P

- password
 - changing (another user) 145
 - changing (one's own) 146
- password criteria
 - setting 62
- passwords
 - changing 61
- post-review preparation phase
 - basic task 19
- preparation phase
 - basic tasks 16
- preset properties
 - adding 22
- preset property
 - adding to service template 103

- definition file 57
- setting 57
- preset property definition file
 - format 57
- process
 - recurring execution 31
- public log 206

Q

- query parameter
 - how to estimate 93

R

- recurring
 - service execution timing 48
 - task categories 47
- recurring task
 - re-registering in a batch 138
- reference information 209
- registering
 - users 61
- registering in JP1/AO
 - user 142
- resolving host names
 - IP addresses 75
- resource group
 - creating 153
 - deleting 155
 - editing 154
- resource groups 66
 - creating 64
 - deleting 64
 - editing 64
 - managing 152
 - relationship to shared service properties 68
 - relationship to user groups 66
- resubmitting
 - tasks 34
- review phase
 - basic task 19
- role
 - set for resource group 68
- roles 67

S

- schedule

- canceling 37, 128
- managing 34, 37
- resuming 37, 127
- suspending 126
- scheduled
 - service execution timing 48
 - task categories 47
- scheduled task
 - re-registering in a batch 138
- service
 - adding 25, 106
 - deleting 25, 109
 - editing 25, 108
 - immediate execution 29
 - managing 25
 - recurring execution 29
 - scheduled execution 29
 - submitting 29
 - submitting for execution at specified time 113
 - submitting for immediate execution 112
 - submitting for recurring execution 114
 - timing of executing 30
- service execution timing
 - immediate 48
 - recurring 48
 - scheduled 48
- service list
 - exporting 25
 - outputting 25
- services
 - executing 111
 - list of JP1/AO services 223
 - managing 105
- service share property
 - setting 139, 140
- service template
 - adding 22, 101
 - adding preset property 103
 - creating 22
 - deleting 102
 - developing 100
 - exporting 104
 - importing 22, 101
 - version 23
- service template list
 - exporting 22
 - outputting 22, 104

- service templates
 - deleting 22
 - managing 22, 99
- setting
 - service share property 139
 - shared service properties 53
 - user information (another user) 143
 - user information (one's own) 144
- shared built-in service properties 53
 - list 54
- shared service properties 53
 - relationship to resource groups 68
 - setting 53
- shared service property
 - note on setting 54
- stopping
 - tasks 34
- SubmitGroup 67
- Submit role 68
- submitting
 - service 29
- submitting service
 - intervening action 27
- system account 62
- resuming suspended task 127
- retrying 44
- retrying from failed step 132
- retrying from step after failed one 133
- step status 50
- stopping 129
- stopping (execution stop) 129
- stopping (forced stop) 130
- suspending 37, 126
- taking time to complete 195
- task categories
 - immediate 47
 - recurring 47
 - scheduled 47
- task executed by logged-in user
 - checking status 38
- task history
 - deleting 135
 - deleting automatically 46
 - retention periods 52
- task list
 - exporting 35, 136
 - outputting 35, 136
- task log
 - displaying 122
 - downloading 123
- task logs 203
- task management
 - overview 35
- tasks
 - categories 47
 - generation timing 47
 - managing 33, 116
 - resubmitting 34
 - retrying 34
 - statuses 48
 - status transitions 48
 - stopping 34
 - stopping forcibly 34
- task summary
 - display format 46
- tasks waiting for response
 - entering actions 124
 - entering responses 124
- task waiting for response
 - action to take 34
 - entering response 34

T

- task
 - archiving 34, 134
 - archiving automatically 45
 - behavior when forcibly stopped 43
 - behavior when stopped 41
 - behavior when stopped while repeated execution plug-ins are running 42
 - canceling 128
 - checking detailed progress in a list 120
 - checking progress 39, 119
 - checking status 38
 - checking status 33
 - checking status (all tasks) 118
 - checking status (logged-in user) 117
 - checking status in flow format 119
 - managing progress 38
 - maximum number of concurrent executions 51
 - moving 34
 - moving to History list 134
 - redoing 131
 - re-executing 131

- time zones
 - daylight saving 32
- Tool Launcher linkage 85
- troubleshooting 192
 - failure to connect to JP1/AO GUI 198
 - task fails to end 196
 - types of problem 193

U

- unlocking
 - user 149
- user
 - deleting from JP1/AO 151
 - locking 148
 - locking and unlocking 61
 - registering in JP1/AO 142
 - unlocking 149
- user authentication method
 - changing 150
- user group
 - assigning resource group 160
 - assigning role 160
 - changing affiliation 161
 - creating 157
 - deleting 162
 - editing 158
- user groups 67
 - allocating resource groups 64
 - allocating roles 64
 - changing affiliation 64
 - creating 64
 - deleting 64
 - editing 64
 - managing 156
 - relationship to resource groups 66
- user information
 - editing 61
 - setting (another user) 143
 - setting (one's own) 144
- User Management permission
 - changing 147
- user management permissions
 - changing 61
- users
 - deleting 61
 - managing 61, 141
 - registering 61

W

- waiting for response task
 - behavior when stopped 42