

Job Management Partner 1 Version 10

**Job Management Partner 1/Automatic Operation
Overview and System Design Guide**

3021-3-312-20(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: 3021-3-312-20(E)

■ **Copyright**

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

Summary of amendments

The following table lists changes in this manual (3021-3-312-20(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 (3021-3-315(E))</i> After the change: <i>Job Management Partner 1/Automatic Operation GUI, Command, and API Reference (3021-3-366(E))</i>	--
Windows Server 2012 R2 was added as an applicable operating system.	--
Linkage with Active Directory is now possible as external authentication linkage.	2.3, 3.2.2, 3.4.3, A.1(1), B
It is now possible to use an API that calls JP1/AO functions from external programs.	2.3
Public key authentication was added as an authentication method used with operation target devices.	3.3.4, 3.4.4
A method to specify whether a user who has logged in is elevated to a superuser was added to the following plug-ins: <ul style="list-style-type: none"> • General command plug-in • File-forwarding plug-in • Content plug-in • Terminal command plug-in 	3.4.4
Evaluations of work folders for operation target devices, and port numbers used by operation target devices, were added.	3.4.5, 3.4.6
Descriptions of debug services and debug tasks were added.	3.4.7, A.3
The HTTPS protocol can now be used to establish a connection between a JP1/AO server and a Web browser.	3.5.2, A.1(1)
Information about the port number (139/tcp) used to establish a connection between a JP1/AO server and target devices was added.	A.1(1)
Information about the port numbers (137/udp and 138/udp) used to establish a connection between a JP1/AO server and target devices was deleted.	A.1(1)

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

Preface

This manual provides an overview of the products and functions of Job Management Partner 1/Automatic Operation and explains the system design.

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

■ Intended readers

This manual is intended for:

- Users who desire an overview of the products and functions of JP1/AO
- Users who are evaluating whether to deploy JP1/AO or who are in charge of system design

■ 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
	Windows Server 2003 R2 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 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, Standard x64 Edition	
	Windows Server 2008	Windows Server 2008 R2	Windows Server 2008 R2 Datacenter	Microsoft(R) Windows Server(R) 2008 R2 Datacenter	
			Windows Server 2008 R2 Enterprise	Microsoft(R) Windows Server(R) 2008 R2 Enterprise	
			Windows Server 2008 R2 Standard	Microsoft(R) Windows Server(R) 2008 R2 Standard	
		Windows Server 2008 x64	Windows Server 2008 Datacenter x64	Microsoft(R) Windows Server(R) 2008 Datacenter x64	
			Windows Server 2008 Enterprise x64	Microsoft(R) Windows Server(R) 2008 Enterprise x64	
			Windows Server 2008 Standard x64	Microsoft(R) Windows Server(R) 2008 Standard x64	
		Windows Server 2008 x86	Windows Server 2008 Datacenter x86	Microsoft(R) Windows Server(R) 2008 Datacenter x86	
			Windows Server 2008 Enterprise x86	Microsoft(R) Windows Server(R) 2008 Enterprise x86	
			Windows Server 2008 Standard x86	Microsoft(R) Windows Server(R) 2008 Standard x86	
		Windows Server 2012	Windows Server 2012 Datacenter		Microsoft(R) Windows Server(R) 2012 Datacenter
			Windows Server 2012 Standard		Microsoft(R) Windows Server(R) 2012 Standard
		Windows Server 2012 R2	Windows Server 2012 R2 Datacenter		Microsoft(R) Windows Server(R) 2012 R2 Datacenter
	Windows Server 2012 R2 Standard		Microsoft(R) Windows Server(R) 2012 R2 Standard		
	Windows Server Failover Cluster				Microsoft(R) Windows Server(R) Failover Cluster
	Windows Vista				Microsoft(R) Windows Vista(R) Business
					Microsoft(R) Windows Vista(R) Enterprise
					Microsoft(R) Windows Vista(R) Ultimate
	Windows XP				Microsoft(R) Windows(R) XP Professional Operating System

#1

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

#2

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

■ Formatting conventions used in this manual

This section describes the text formatting 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 6

1 Overview of JP1/AO 11

1.1 Challenges faced in system operations 12

1.2 Benefits of deployment 13

1.3 Example application of JP1/AO 15

1.3.1 Operation procedure using JP1/AO 16

1.4 User operations and approach to automation in JP1/AO 17

2 Introduction to functions 19

2.1 Functions for automating operation procedures 20

2.2 Functions for managing operation targets 22

2.3 Functions for linking with other products 24

3 Designing a JP1/AO system 29

3.1 JP1/AO system lifecycles 30

3.2 Design procedure 32

3.2.1 Service design procedure 32

3.2.2 Operation design procedure 33

3.2.3 System design procedure 34

3.3 Service design 35

3.3.1 Evaluating the service template to be used and the targets of operation 35

3.3.2 Evaluating the items to be considered when services are added 35

3.3.3 Evaluating the items to be specified when services are run 36

3.3.4 Evaluating the shared service properties 37

3.4 Operation design 39

3.4.1 Evaluating users and access permissions 39

3.4.2 Evaluating operations using groups 40

3.4.3 Evaluating operations using external authentication linkage 40

3.4.4 Evaluating operations for access control by device 41

3.4.5 Evaluating the work folders for target devices 42

3.4.6 Evaluating port numbers used for target devices 43

3.4.7 Evaluating the task retention period 43

3.4.8 Evaluating the status notification method 44

3.4.9 Evaluating maintenance 45

3.4.10	Evaluating error handling	45
3.4.11	Evaluating audit logs	46
3.5	System design	47
3.5.1	Evaluating the system configuration	47
3.5.2	Evaluating the network settings	49
3.5.3	Checking the operating environment	50
3.5.4	Evaluating the details of installation	50

Appendixes 51

A	Reference Information	52
A.1	Lists of port numbers	52
A.2	Prerequisites for connection destinations	54
A.3	List of limit values of functions	56
A.4	Version changes	57
A.5	Reference material for this manual	57
B	Glossary	62

Index 68

1

Overview of JP1/AO

JP1/AO is a product for automating the operation of systems that are constantly improving and becoming more complex.

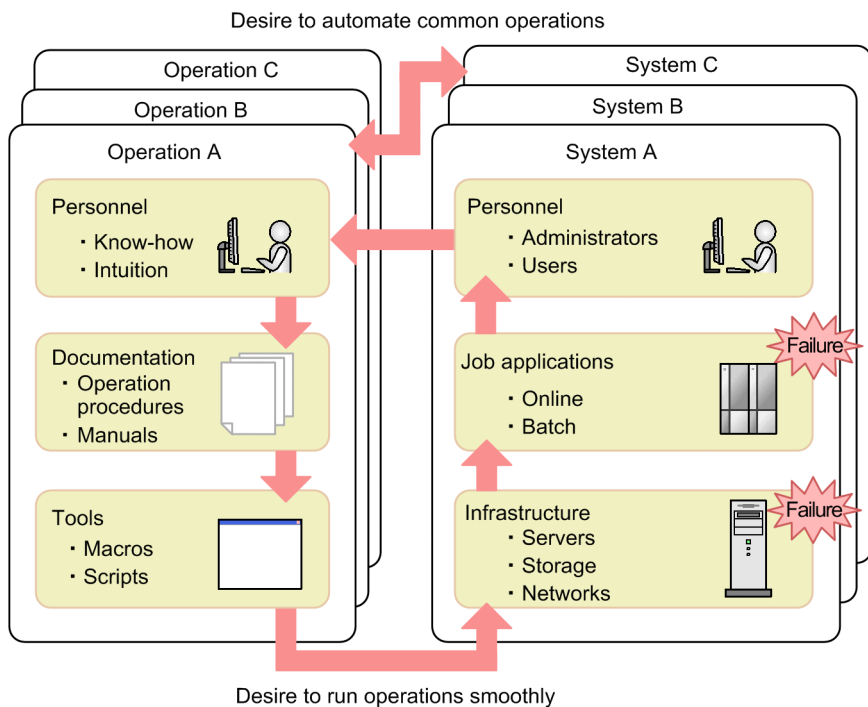
This chapter provides an overview of JP1/AO.

1.1 Challenges faced in system operations

System operations are becoming increasingly complex.

To run a system, you need documentation (operation procedures and manuals), tools (macros and scripts), and the know-how and intuition of experienced administrators. In addition, due to the increasing use of cloud data centers and the increasing development of virtualization technology, office systems are becoming larger and moving in the direction of operations that consolidate multiple systems. Even in consolidated systems, complexity is further increasing because of the requirement to support operations that are specific to individual systems.

Figure 1–1: Challenges faced in system operations



In the field of system operations, there are currently large numbers of operation procedures, which adds significantly to the workload of the personnel involved. To improve this situation, measures are required to reduce the tasks that depend on manpower and to improve operational efficiency.

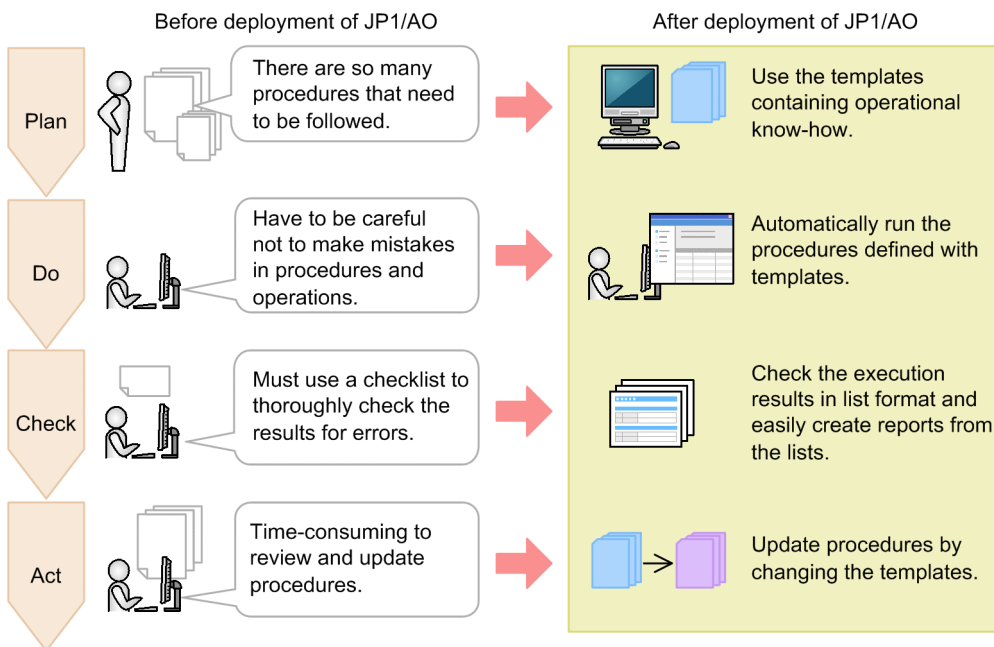
1.2 Benefits of deployment

Deploying JP1/AO provides a means to resolve problems associated with the operation of consolidated systems.

- Improvement in operational efficiency and reduction in human errors
In traditional system operations, the operators run multiple software programs by using multiple operation procedures. JP1/AO can reduce such labor-intensive tasks. JP1/AO can also reduce the incidence of human errors because it processes operation procedures automatically. This means that more time is available for running system operation tasks and that operators can focus on making improvements to the operating methods, thereby increasing the rate at which you are able to improve operations.
- Easy deployment and standardized operations
JP1/AO provides *typical operation procedures* that are derived from various types of operational know-how, such as cloud data centers and office systems. These typical operation procedures are provided as ready-to-use templates. When you apply these templates to multiple system operations, you also promote standardization of operations.

The following explains how the deployment of JP1/AO benefits each phase of the Plan, Do, Check, Act system operation cycle.

Figure 1–2: Benefits of JP1/AO deployment



- Plan (design and develop operations)
Traditionally, operational know-how that has been accumulated over many years has been documented in procedure manuals. These procedure manuals are organized by system, and need to be repeatedly revised individually. JP1/AO provides operational know-how in the form of templates. These templates enable you to apply a standard operation procedure to multiple systems by entering into templates the information that is unique to each system, such as a server name.
- Do (operate)
Traditionally, the operators must run various products that are needed for operations by referencing a large number of procedure manuals. The operators must also avoid human errors, such as errors in following the procedures and in skipping required operations.

If you deploy JP1/AO and use the operation procedures defined in templates, you can run various products automatically. JP1/AO also supports date-and-time-specified execution and periodic execution. You can reduce human errors, such as errors in following procedures and in skipping required operations.

- Check (check operation results)

Traditionally, the user must check the execution results against a large number of checklists.

JP1/AO enables the user to check the results of automatic processing in a list window. Because such lists can be exported as execution logs, the user can also create reports of operation results efficiently.

- Act (re-evaluate operation)

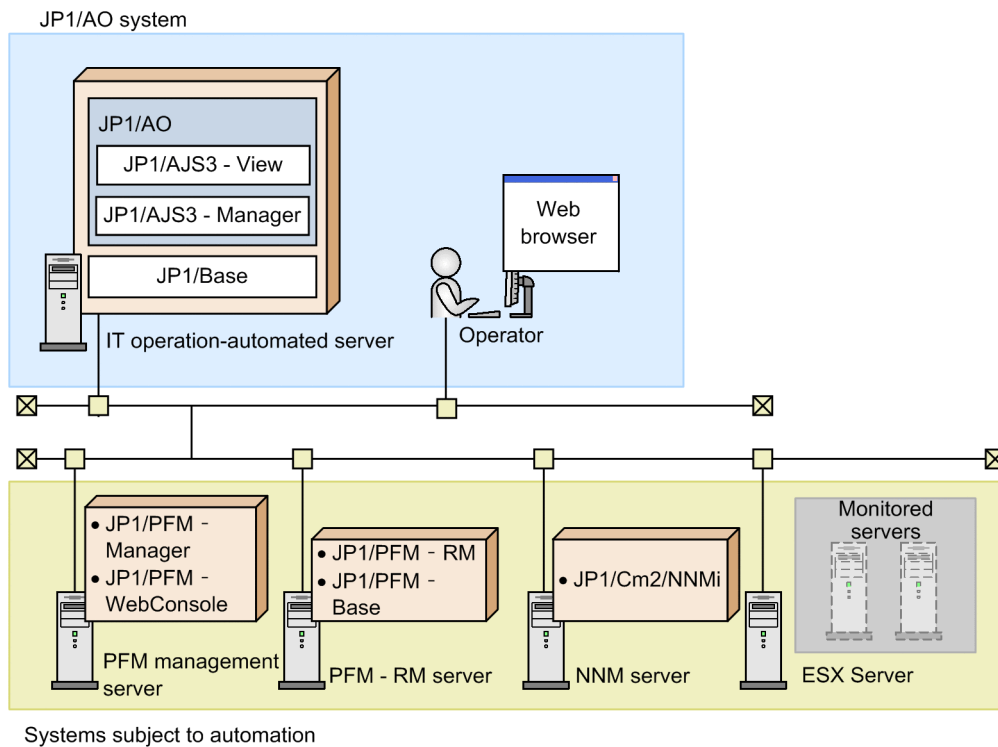
Traditionally, the user must update the operation procedures each time the system configuration is changed.

In an environment where JP1/AO is deployed, the user can update the operation procedures by upgrading the templates. Improving procedures requires the know-how of administrators and operators. The resources and efforts required to improve procedures are made available by the improved efficiency of Plan, Do, and Check. The user can also efficiently determine guidelines for how and where to improve because those operation procedures that are most error-prone and those that are most frequently used can be identified by analyzing the execution logs.

1.3 Example application of JP1/AO

JP1/AO automates operation procedures. JP1/AO automates not only operations of JP1 products but also of OSs, such as Windows and UNIX. This section explains an example application of JP1/AO based on the *Add monitoring settings* template for JP1 products.

Figure 1–3: System configuration for an example application



JP1/AO system

- IT operation-automated server
This is the server whose operation procedure is to be automated. JP1/AO and the prerequisite products are installed on this server.
- Web browser
This is the terminal used to operate JP1/AO by means of a Web browser. The operator who will be automating the operation procedure uses this terminal.

Systems subject to automation

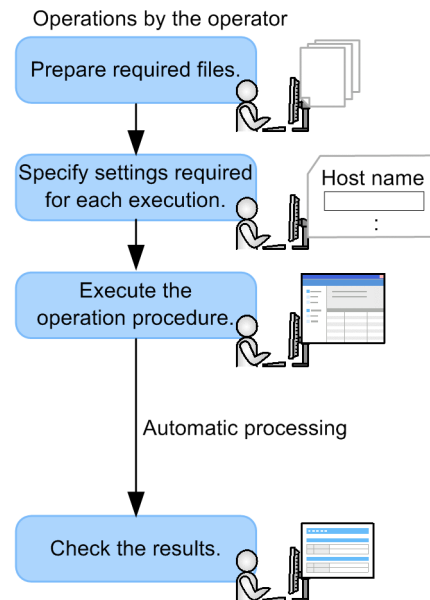
- PFM management server
Summarizes the operating information received from the PFM - RM server and displays it in JP1/PFM's monitoring window. JP1/PFM - Manager and JP1/PFM - WebConsole are installed on the PFM management server.
- PFM - RM server
Collects the operating information subject to monitoring and sends it to the PFM management server. JP1/PFM - RM for Platform and JP1/PFM - Base are installed on this server.
- NNM server
Centrally manages a multi-vendor network. JP1/Cm2/NNMi is installed on this server.
- Monitored servers

Servers to be added as monitored targets to JP1/PFM and JP1/Cm2/NNMi. In this example, two virtual servers on ESX Server are the monitored servers.


1.3.1 Operation procedure using JP1/AO

The following describes an operation procedure that uses the *Add monitoring settings* template. The procedure explained here uses a Web browser.

Figure 1–4: Operation procedure using JP1/AO



Legend:

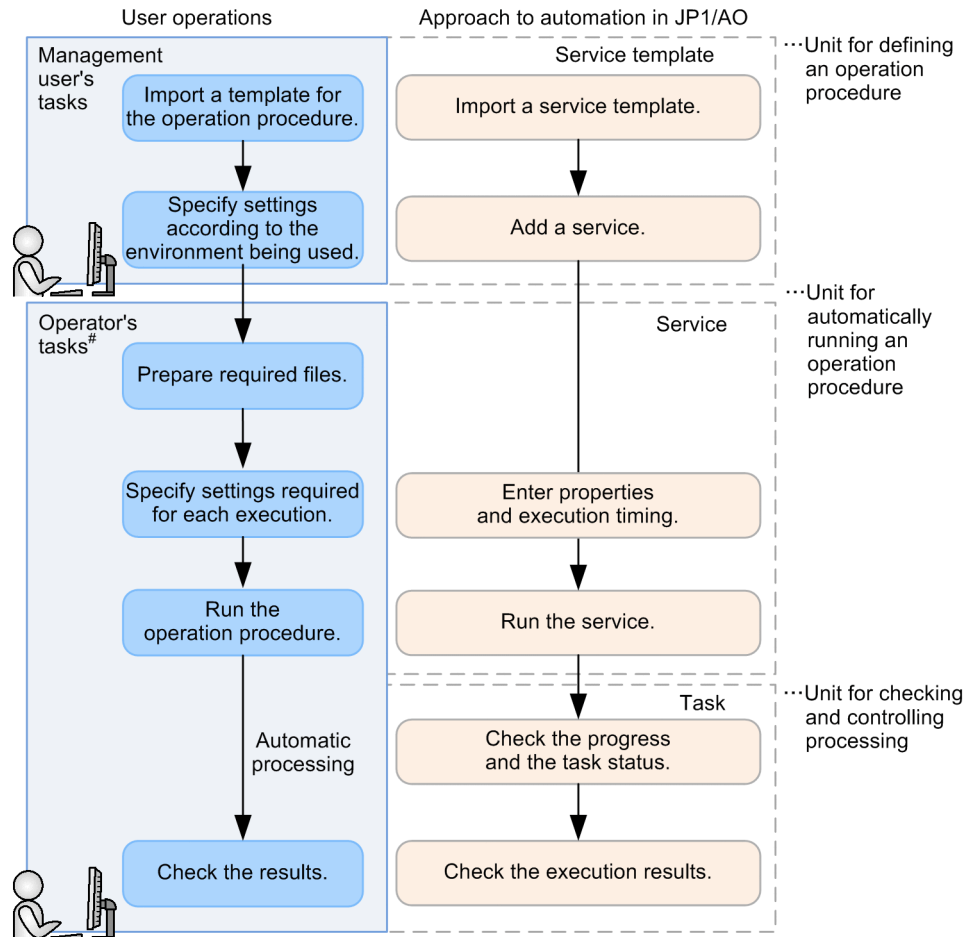
 : User operation

1. In the JP1/AO system, prepare the files that are required for adding targets to be monitored.
In *Add monitoring settings*, prepare JP1/PFM's monitored target definition file. Also prepare other files as necessary, such as an agent hierarchy definition file and an application definition file.
2. Specify the information required for a template for *Add monitoring settings*.
Specify the required information, including the host names of the PFM management server, PFM - RM server, NNM server, and monitored servers, and the IP addresses of the virtual servers that are to be added as monitored targets. If necessary, you can also specify execution timing (execution date and time and a repetition interval).
3. Execute the operation procedure defined in the template.
The specified operation procedure is processed automatically.
The step in which two virtual servers are added as monitored targets of JP1/PFM and JP1/Cm2/NNMi is processed automatically. The files you prepared in step 1 are automatically transferred to the PFM management server.
4. Check the results of automatic processing in the list window.
If `Completed` is displayed in the JP1/AO window, automatic processing was successful.
If `Failed` is displayed, automatic processing has failed. Output the log information to check the processing results and eliminate the cause of the error. You can then perform the processing again.

1.4 User operations and approach to automation in JP1/AO

This section explains the user operations and the approach to automating operation procedures. The users include a management user who imports operation procedure templates into JP1/AO and specifies environment-specific settings, and an operator who handles operation procedures.

Figure 1–5: User operations and approach to automation in JP1/AO



Legend:

- : User operation
- : Operation in the JP1/AO system
- : JP1/AO system element

Note: For details about the operation example, see 1.3.1 *Operation procedure using JP1/AO*.

Management user's tasks

1. Import into JP1/AO a template for the operation procedure (import a service template).
JP1/AO provides various templates (service templates) that define operation procedures. Service templates become available as services when they are imported into JP1/AO.
2. Enter into the service template information specific to the environment being used (add a service).
Enter environment-specific information into the imported service template and add this to JP1/AO as a service. Beginning with a single service template, you can add multiple services suitable for different operation procedures and tasks.

Operator's tasks

1. Prepare the files required for processing.
Once you prepare these files, you can transfer them to the operation targets automatically when you use JP1/AO to process operation procedures automatically.
2. Specify the settings required for each execution (enter properties and execution timing).
You can specify the settings required for an operation procedure template by entering properties and execution timing information in the JP1/AO window.
3. Run the operation procedure (run the service).
The operation procedure is processed automatically. You can check the progress and status of the executed operation procedure as *tasks* in the JP1/AO window.
4. Check the results of automatic processing.
When the processing is finished, you can check the JP1/AO window to see whether the processing terminated normally. If the processing failed, you can check for the processing that resulted in an error.

Elements of a JP1/AO system

The templates for operation procedures used in JP1/AO change from *service templates* to *services* to *tasks* at the different stages of the operation.

- Service template
The template for an operation procedure used in JP1/AO is called a *service template*.
- Service
A service template that has been imported into the JP1/AO system together with the environment-specific information that has been entered is called the *service*. You process an operation procedure automatically by executing a service.
- Task
When the information required for execution is specified and then the service is executed, a *task* is generated. To check the progress and results of automatic processing, check the status of the task.

Related topic

- [1.3.1 Operation procedure using JP1/AO](#)

2

Introduction to functions

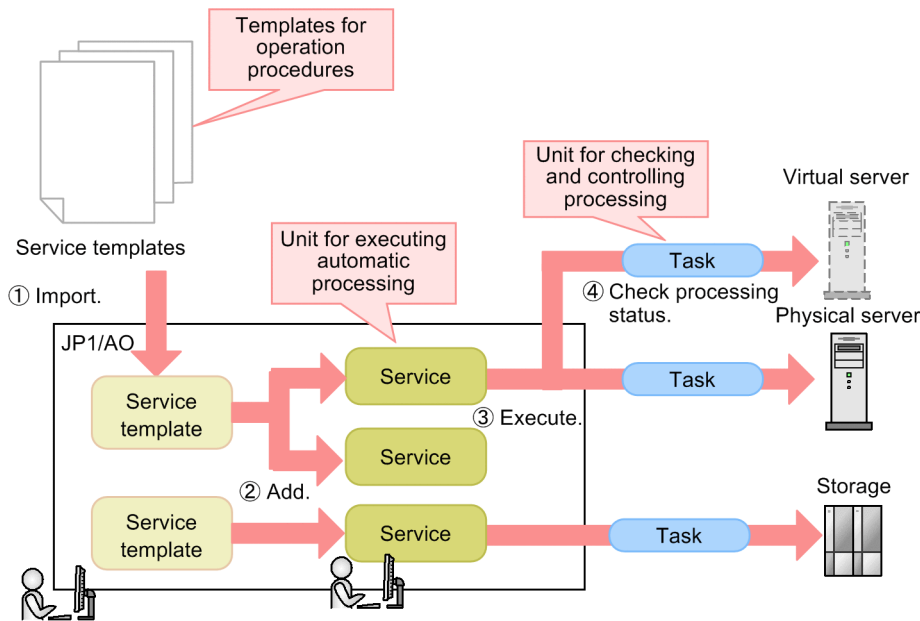
JP1/AO provides *functions for automating operation procedures* that enable you to define and perform automatic processing, and *functions for managing operation targets* that enable you to manage users and the hosts at the connection destinations. It also provides *functions for linking with other products* that enable you to send email notifications in the event of errors and to use direct access URL to display a target window. This chapter provides an introduction to these functions.

For details about the functions, see the *Job Management Partner 1/Automatic Operation Administration Guide*.

2.1 Functions for automating operation procedures

You use JP1/AO to automate operation procedures. This section explains the procedure for automating operation procedures and provides an introduction to the principal functions needed to achieve automation.

Figure 2–1: Procedure for automating operation procedures



- ① Import a service template that defines an operation procedure.
- ② Enter information into the service template, and add the service template to create services.
- ③ Enter information such as the execution timing, and then run the services.
- ④ Use the generated tasks to check the processing status.

Providing a wide variety of templates that define operation procedures - managing the service templates

JP1/AO provides various templates (called *service templates*) that define operation procedures.

The user selects job-appropriate templates and imports them into JP1/AO. When templates are imported, their automated operation procedures can be used as services.

In addition to using the templates provided by JP1/AO as they are, the user can modify them to create new service templates in which to define user-specific operation procedures.#

#

User-created service templates that are not based on those provided by JP1/AO (JP1/AO standard package and JP1/AO Content Set) are not supported. However, plug-ins provided by JP1/AO (JP1/AO standard package and JP1/AO Content Set) that are called from such unsupported service templates are supported.

Creating services that are suitable for operation procedures and jobs - adding services

You develop a service by entering environment-specific information into an imported service template and adding the service template to JP1/AO as a service. You can create multiple services suitable for your various operation procedures and jobs from a single service template.

Scheduling according to jobs - running services

You enter the information necessary for running a service and the execution timing, and then run the service. When a service is run, a task is generated and the automatic processing is started at the date and time that you have specified. JP1/AO supports (as execution timings) immediate execution, repeated executions on a specified day of every week or at the end of each month, and date-and-time-specified executions for executing services on a specified date and time. This allows you to set a detailed schedule tailored to your business needs.

Using task lists to check the processing status and the details window to check the progress of each job - managing tasks

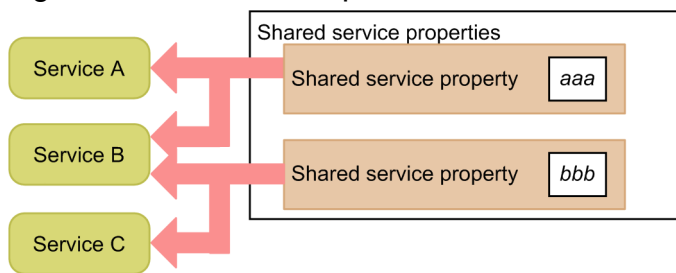
JP1/AO provides task lists that enable you to determine the processing status at a glance and a details window that enables you to check the progress of each job and output task logs. If you use a plug-in (the User-response wait plug-in) that enables the user to select the subsequent processing on the basis of the current processing results, you can enter the appropriate information to a task during processing, as necessary.

Sharing settings to reduce the time and effort needed in entering and changing settings - managing shared service properties

JP1/AO enables you to share the values specified for a service among multiple services. Settings that are shared are called the *shared service properties*.

For example, if you use a service template to manage a common server and you define the host name, user ID, and password for that server at the connection destination as shared service properties, you save the time needed to enter this server information each time a service is run.

Figure 2–2: Relationship between shared service properties and services



Classifying operation targets by jobs, groups, and usages - setting categories

You can classify services and tasks by usage and type categories and display them in a hierarchical structure.

Because JP1/AO enables you to register the same service in multiple categories, you can display a list of services according to purpose, such as for checking services by job or by the person in charge.

2.2 Functions for managing operation targets

JP1/AO provides the following functions to manage operation targets:

- Managing groups

You can use user groups and resource groups to restrict the range of services that can be run and tasks that can be referenced for each user group.

- Managing connection destinations

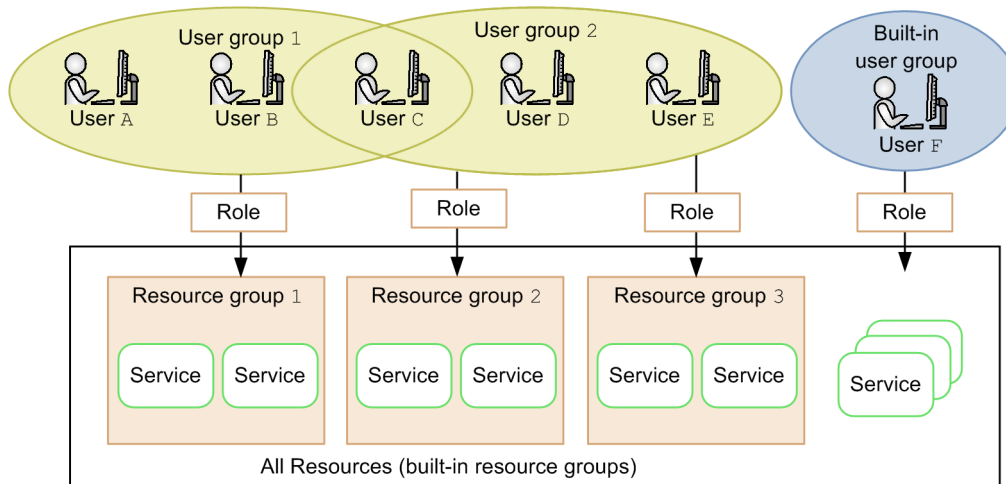
In JP1/AO, a host at a connection destination that is the operation target of a service is called a *connection destination*. You can restrict connection destinations as targets of services for each resource group, and centrally manage authentication information for hosts at connection destinations in order to reduce workload during operation.

Detailed access control according to operations and jobs - managing groups

By allocating resource groups to user groups, you can restrict the services and tasks that each user can access. At this time, you can specify permissions (roles) to restrict available service operations (such as managing and running services) for each user group.

The following shows an example of access control using resource groups and user groups.

Figure 2–3: Access control using resource groups and user groups



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

Thus, using group management enables you to efficiently control accessible services so that they match the usage goals of users.

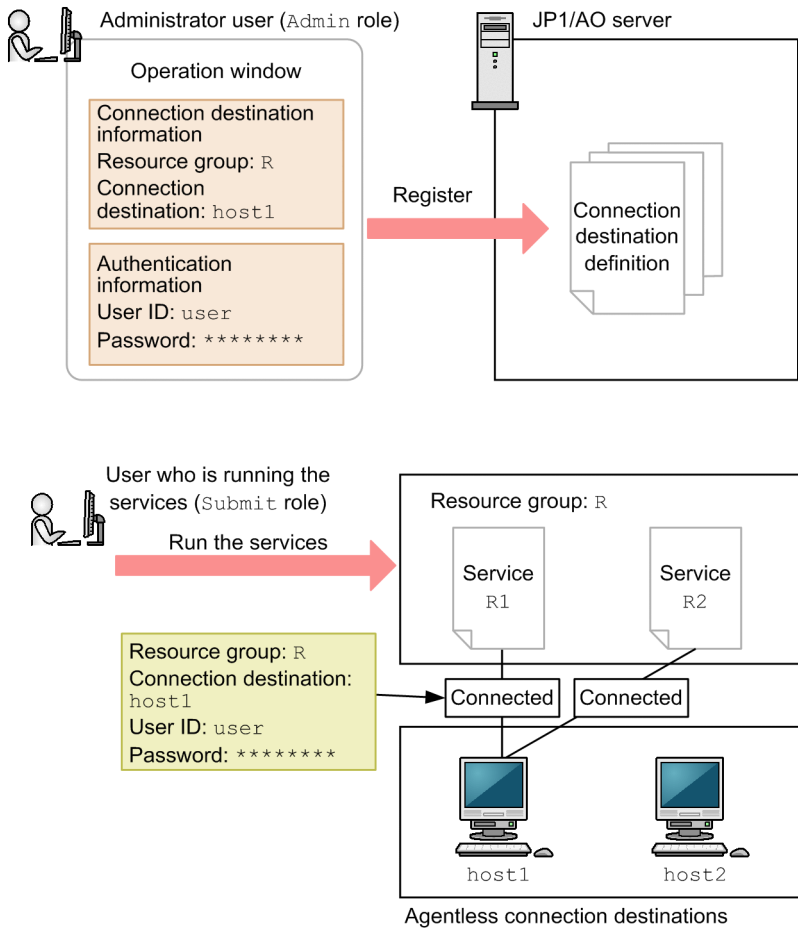
For example, if IT operations running at a data center are divided among multiple tenants, you can classify the services used by the individual tenants by resource group and restrict the services that can be run by each user group. This allows you to prevent services of another tenant from being run by mistake, and to restrict the range of tasks that can be referenced by each tenant.

Agentless operations that reduces the load of management - managing connection destinations

The function for managing the connection destination information (including resource group names and host names) and the authentication information (including the user ID, password, and protocol used to log in to the host at the connection destination) for each connection destination is called the *connection destinations management function*.

If you register the connection destination information in JP1/AO, you can control accesses to the connection-destination hosts for each resource group when running services. If you also register the authentication information, you can save the time required to enter the authentication information each time a service is run because JP1/AO can manage information (such as passwords) shared among multiple services. You can also specify the protocol and authentication method for each host to be connected.

Figure 2–4: Example of agentless connection



In this figure, the administrator user with the Admin role uses window operations to register connection destination information and authentication information, and then the service execution user with the Submit role for resource group R runs the services. In this case, the service execution user can connect only to host1 whose connection destination information has been registered, but cannot connect to any other host. Because the authentication information for host1 has been registered in JP1/AO, the user does not need to enter a user ID or password when running a service.

2.3 Functions for linking with other products

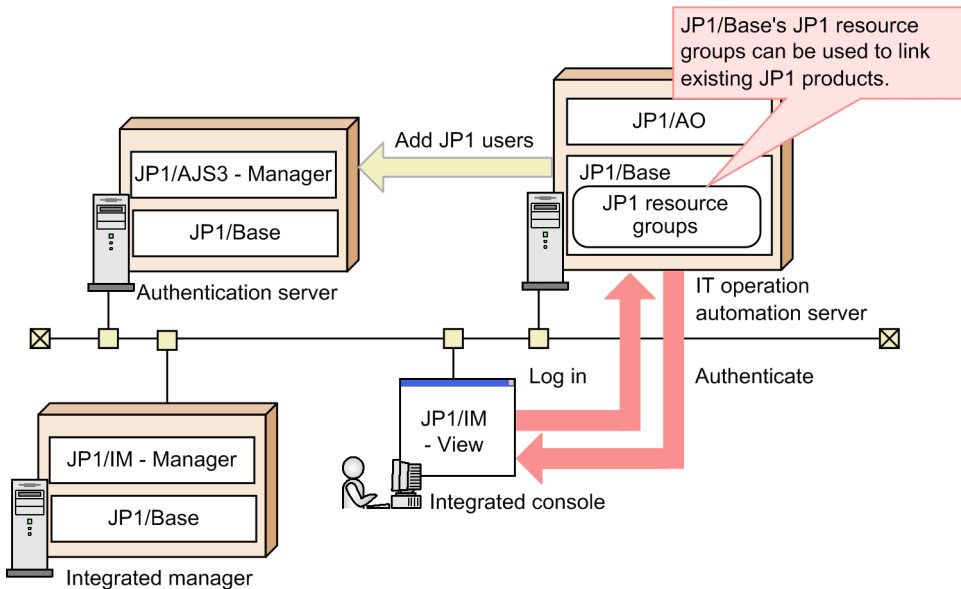
JP1/AO provides functions for improving the work efficiency of administrators, including email notifications when errors occur, a direct access URL that enables target windows to be displayed directly, and an API that calls JP1/AO functions from external programs.

Taking advantage of existing JP1 resource groups - linking with JP1/Base's authentication function

JP1/AO enables you to use JP1/Base's authentication function to manage JP1/AO's user accounts. If you link your JP1/AO with JP1/Base, there is no need to manage users and user groups in JP1/AO. You can also use the existing JP1 users.

To use JP1/Base to manage users, you use JP1/Base window operations to create JP1 users and to specify JP1 resource group names and permission levels. If you specify JP1 resource group names and permission levels that match the resource group names and permissions in JP1/AO, you can manage those users as JP1/AO users.

Figure 2–5: Linking with JP1/Base's authentication function



Using Active Directory to manage users and groups - linking with Active Directory

Linking JP1/AO with Active Directory[#] allows Active Directory to perform user authentication. In other words, Active Directory users can log in to JP1/AO.

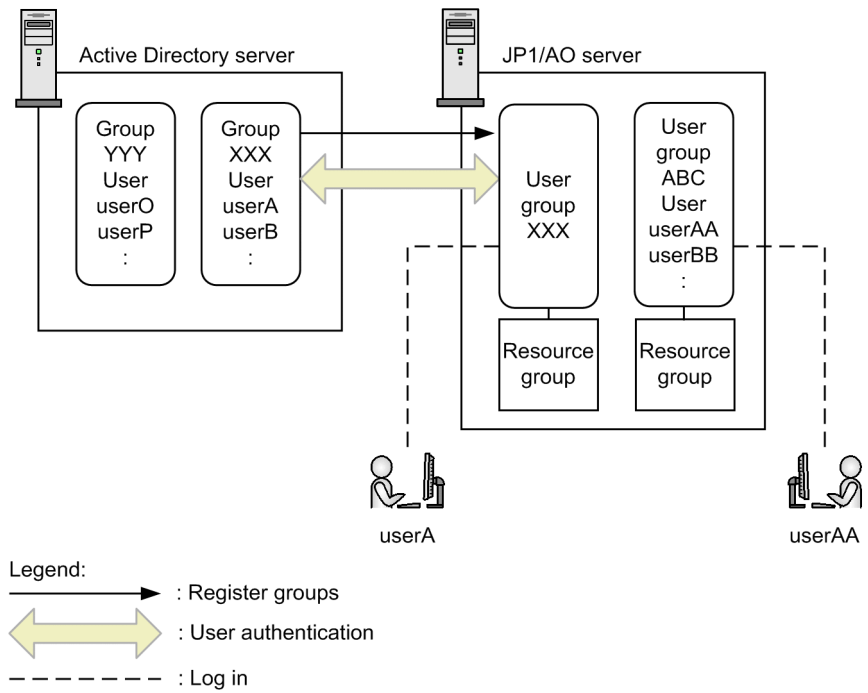
To link JP1/AO with Active Directory, you can select whether to link groups.

If you do not link groups, JP1/AO manages user groups and resources and Active Directory performs user authentication. You need to register the same users in both JP1/AO and Active Directory, but register passwords only in Active Directory.

If you link groups, an Active Directory group that contains a user who logs in to JP1/AO must be registered as a JP1/AO user group. Then, Active Directory performs user authentication. Active Directory manages users in the groups, and JP1/AO manages resources for the groups. Therefore, there is no need to register a user in JP1/AO.

[#] This linkage can be used if JP1/AO uses Active Directory as an LDAP directory server.

Figure 2–6: Linkage with Active Directory (when linking groups)



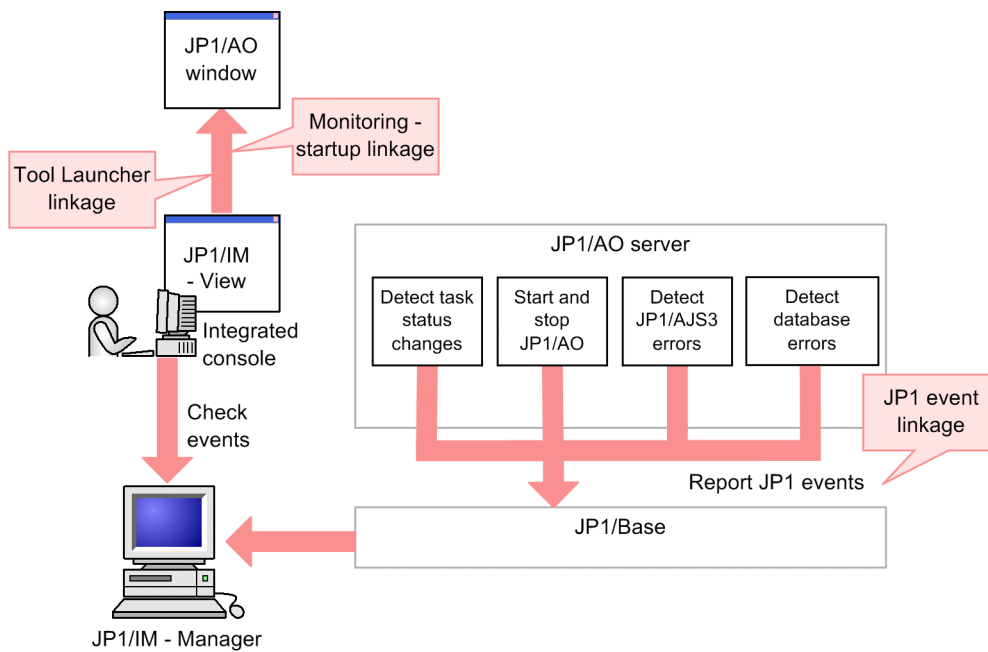
System monitoring linked with JP1/IM - linking with JP1/IM's event monitoring function

JP1/IM achieves integrated system management by linking JP1-series products, including job management and storage management, and other middleware products, as well as managing the configuration and operation of the overall system.

The following features become available when you link your JP1/AO with JP1/IM:

- JP1 event linkage, which enables you to use JP1/IM to centrally manage the JP1 events issued by JP1/AO
- Monitoring-startup linkage, which enables you to define windows to be displayed in JP1/IM - View and then display the associated JP1/AO windows from JP1 events
- Tool Launcher linkage, which enables you to connect to the JP1/AO windows from JP1/IM - View

Figure 2–7: Linking with JP1/IM's event monitoring function

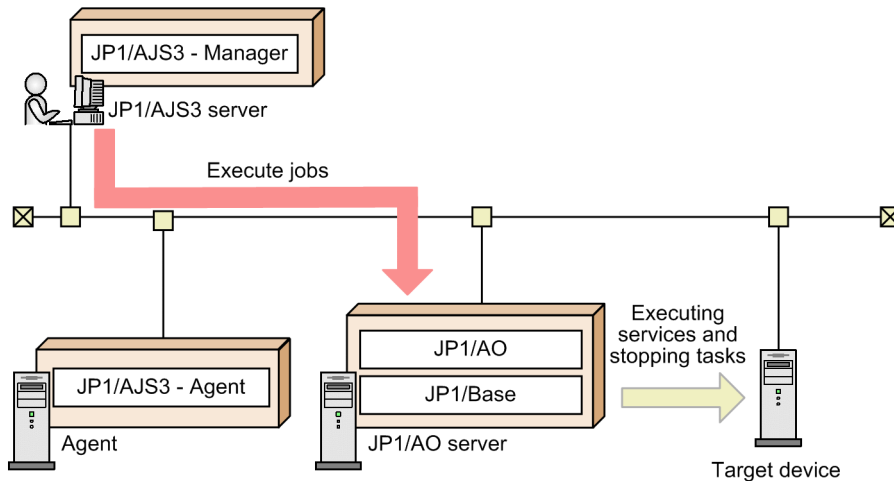


Executing services and stopping tasks from JP1/AJS3 - linking with JP1/AJS3

Linking with JP1/AJS3 lets you automatically execute the following commands on the JP1/AO server from the JP1/AJS3 server:

- `submittask` command (executing services)
- `stoptask` command (stopping execution of tasks)

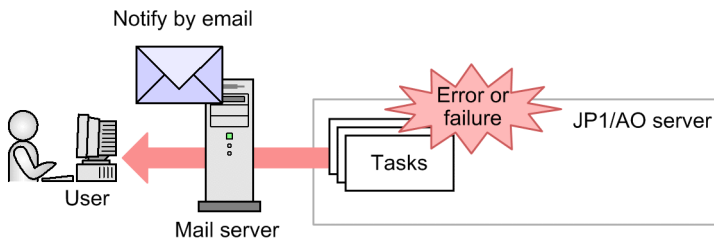
Figure 2–8: Linking with JP1/AJS3



Streamlined error detection - email notification

If the status `Abnormal Detection` or `Failed` is detected in a task that is being processed, the event can be reported by email. Because the email that is sent can include the URL of the details window for the failed task, you can reduce the time required to handle the error once the email is received.

Figure 2–9: Email notification

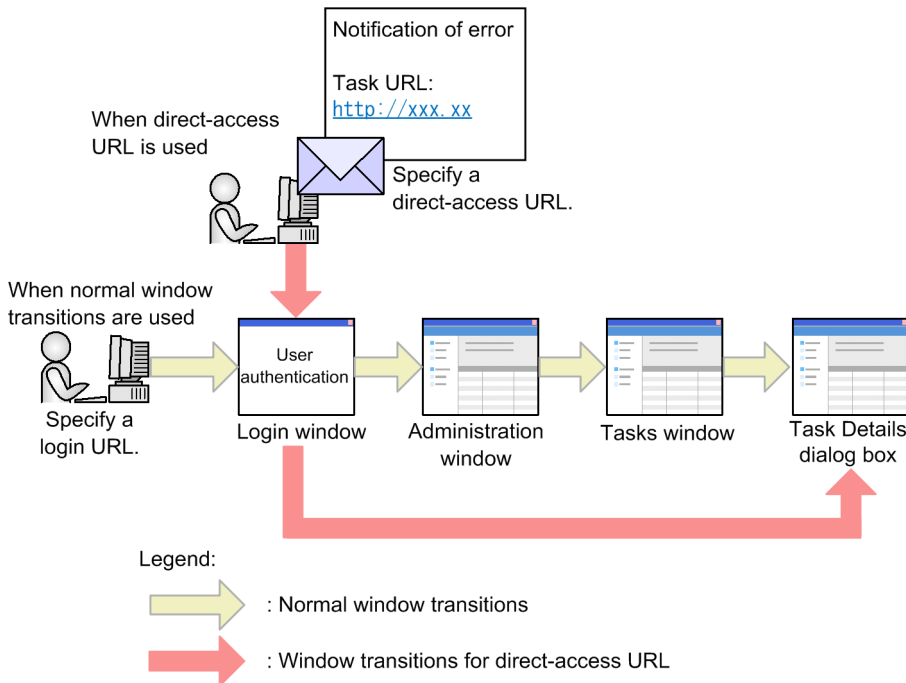


Improving work efficiency by directly accessing a target window - direct-access URL

JP1/AO provides the direct-access URL function that enables you to go directly to the target window as soon as you have logged in.

When you use the normal window transitions, it takes time to find the target from a list of services and tasks after you log in. By using the direct-access URL, you can display a service execution window, a service setup window, or a task details window immediately after you log in.

Figure 2–10: Direct-access URL

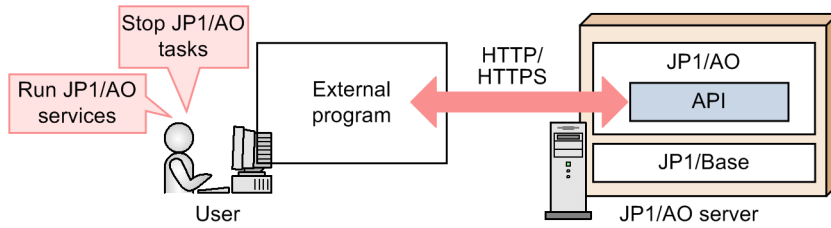


Calling JP1/AO functions from external programs - API

You can use an API to call JP1/AO functions from an external program. For example, you can run services and stop tasks from an external program without using JP1/AO windows. The API uses the HTTP or HTTPS protocol for communication.

For details, see *API* in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*.

Figure 2–11: API



Single sign-on to Hitachi Command Suite products - Link & Launch setting

You can start any Hitachi Command Suite product from a JP1/AO window with a single sign-on. This enables you to enter property values for a service that is running while checking a Hitachi Command Suite product's window. Note that the Hitachi Command Suite products that can be started from JP1/AO must be installed on the same server where JP1/AO is installed.

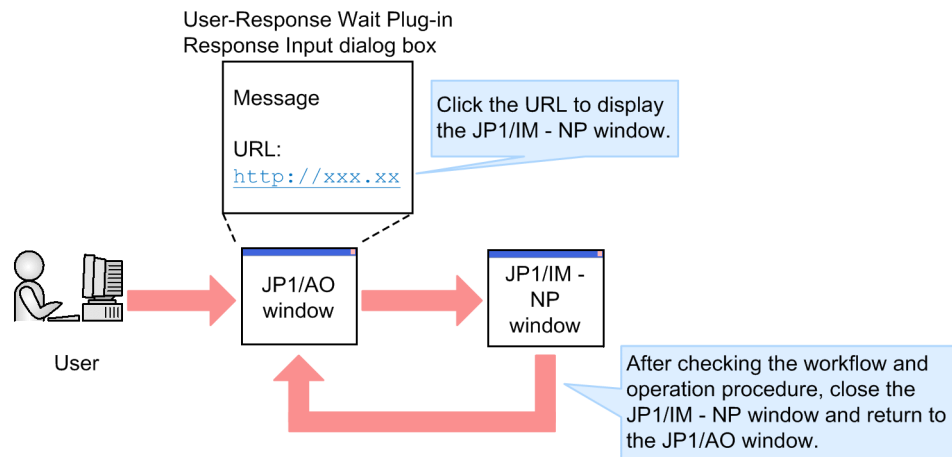
You can apply the Link & Launch function to the following products:

- Hitachi Device Manager Software
- Hitachi Tuning Manager Software
- Hitachi Global Link Manager Software
- Hitachi Replication Manager Software
- Hitachi Compute Systems Manager Software

Single sign-on to a JP1/IM - NP window - Linking with JP1/IM - NP job contents

You can start a JP1/IM - NP window from a JP1/AO window with a single sign-on. In the **Respond** dialog box, you can view the JP1/IM - NP job contents (business flow and guide) to check workflow and operation procedures.

Figure 2–12: Linking with the JP1/IM - NP job contents



3

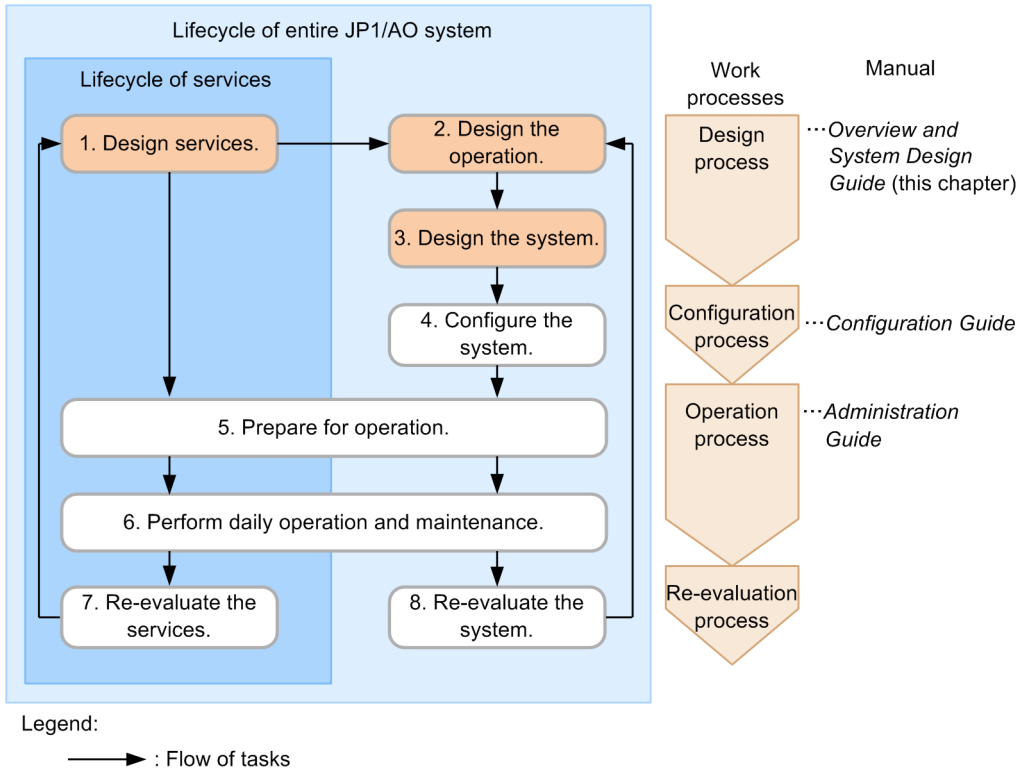
Designing a JP1/AO system

This chapter explains the lifecycles of a JP1/AO system and the evaluations required when a JP1/AO system is designed.

3.1 JP1/AO system lifecycles

There are two lifecycles in a JP1/AO system, which differ in terms of purpose and frequency of use. One is the lifecycle of a service, which is the execution unit of IT operation, while the other is the lifecycle of the entire JP1/AO system that supports the operation of the services.

Figure 3–1: Lifecycle of an IT operation (service) and lifecycle of the entire JP1/AO system (with manual references)



A lifecycle consists of four processes, which are the design process, the configuration process, the operation process, and the re-evaluation process. The following explains the tasks involved in each process.

Design process

1. Design services

Identify the IT operations to be automated and evaluate the requirements for the services and the method of running the services (including execution schedules and categories).

2. Design the operation

Evaluate how to run the JP1/AO system, such as users' roles and error notification methods, according to the IT operations to be automated.

3. Design the system

Evaluate the system configuration, including the configuration of the JP1/AO system and the network settings, based on the details of the service and operation designs.

Configuration process

4. Configure the system

Install JP1/AO and perform the various setup steps based on the details evaluated in the system design.

Operation process

5. Prepare for operation

Prepare the services and the users required for running the services and the JP1/AO system based on the details evaluated in the service and operation designs.

- Preparing for running the services
Add the services corresponding to the IT processing targets to the JP1/AO system.
- Preparing for running the JP1/AO system
Perform various setup steps, including the users for logging in to JP1/AO, the mail server required when the services run, and the SMTP server.

These tasks are performed on the configured JP1/AO system using window operations and commands.

6. Perform daily operation and maintenance

- Operation related to services
Run and manage the services (including management of tasks) as daily operations.
- Operation related to JP1/AO system
Perform the JP1/AO system maintenance tasks (including making backups) as needed.

Re-evaluation process

7. Re-evaluate the services

To improve the efficiency of automatic processing and to increase the number of targets to be processed automatically, re-evaluate the operating status after you have run the system for a while. For example, analyze service operation efficiency on the basis of the service execution logs and re-evaluate whether the efficiency of frequently used services can be improved and whether more IT operations can be automated.

As a result of re-evaluation, perform the tasks again, starting with design of services, if any element needs to be augmented or modified.

8. Re-evaluate the system

Re-evaluate the JP1/AO system as necessary in response to changes to the configuration and the size of the system. As a result of re-evaluation, perform the tasks again, starting with design of operation, if any element needs to be augmented or modified.

This chapter explains the design process. For details about the other processes, see the corresponding manuals.

Related topics

- [3.3 Service design](#)
- [3.4 Operation design](#)
- [3.5 System design](#)

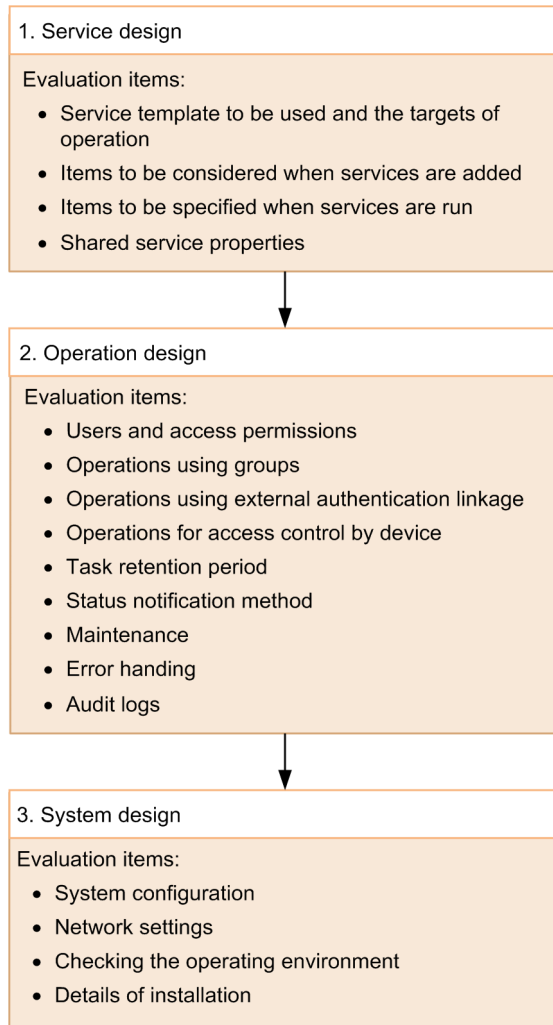
3.2 Design procedure

In JP1/AO, the design process consists of service design for evaluating the services needed in order to automate IT operations, operation design for running the services efficiently, and system design for configuring the system based on the operation design.

This section explains the design procedure and what needs to be evaluated during the design process.

The following figure shows the basic design procedure in JP1/AO.

Figure 3–2: Basic design procedure in JP1/AO



Related topics

- [3.1 JP1/AO system lifecycles](#)

3.2.1 Service design procedure

Service design involves the following tasks:

1. Evaluating the service template to be used and the targets of operation

Evaluate the service templates and select the one that would be suitable for the purpose of the IT operation. Also check the operating environments for the devices that are the operation targets when services are run.

2. Evaluating the items to be considered when services are added

Evaluate the definition items, including categories and properties, that are to be specified when services are added.

3. Evaluating the items to be specified when services are run

Evaluate the information, including execution timing and properties, that is to be specified at the time of execution by the users who run the services.

4. Evaluating the shared service properties

Evaluate the values for service properties that can be shared among services.

Related topics

- [3.3 Service design](#)

3.2.2 Operation design procedure

Operation design involves the following tasks:

1. Evaluating users and access permissions

Evaluate the management of users and user groups and the granting of permissions according to user roles.

2. Evaluating operations using groups

Evaluate multi-tenant operations that use resource groups so that accesses to services can be restricted by user group.

3. Evaluating operations using external authentication linkage

Evaluate use of JP1/Base or Active Directory for management of users.

4. Evaluating operations for access control by device

Evaluate access control for the target devices when services are run and the management of connection destination information and authentication information.

5. Evaluating the task retention period

Evaluate the retention periods from task completion to task archiving and from task archiving to task deletion.

6. Evaluating the status notification method

Evaluate how to report the status of the system and of tasks. Available methods include use of email and event notification.

7. Evaluating maintenance

Evaluate system backup and database reorganization as elements of periodic maintenance procedures.

8. Evaluating error handling

Evaluate how to handle errors, including how to collect data in the event of a failure during JP1/AO system operation.

9. Evaluating audit logs

Evaluate audit logs, including whether audit logs are to be issued and the number and size of audit files.

Related topics

- [3.4 Operation design](#)

3.2.3 System design procedure

System design involves the following tasks based on the results of operation design:

1. Evaluating the system configuration

Evaluate the appropriate JP1/AO system configuration for the operations, such as a basic configuration, a cluster configuration, or a system configuration linked with JP1/IM.

2. Evaluating the network settings

Evaluate the networks between the JP1/AO server and the Web browser and between the JP1/AO server and the target devices.

3. Checking the operating environment

Evaluate the JP1/AO system operating environment.

4. Evaluating the details of installation

Evaluate the settings to be specified when you install JP1/AO.

Related topics

- [3.5 System design](#)

3.3 Service design

You identify in the service design the IT operations to be automated, and then you evaluate the service templates to be used and the service running methods (including execution schedules and categories).

3.3.1 Evaluating the service template to be used and the targets of operation

Analyze the current operation procedures and evaluate the following items when you have determined the operation procedures that are to be automated:

- Service templates to be used
JP1/AO provides as the JP1/AO standard package and the JP1/AO Content Set various types of service templates, including service templates that support setup, operation, and error handling of various JP1 products, virtual server operations, and cloud operations. If you want to automate your system operations without using these JP1/AO-provided service templates, consider creating service templates. You can create a new service template, or copy and edit a service template provided by JP1/AO.
- Target devices when services are run
After you have decided the service template to be used, check whether its prerequisites are satisfied by the operating environments of the target devices that will perform the IT operations automatically, such as the servers and storage. For details about the prerequisites for service templates, see the descriptions of the prerequisites for the individual service templates in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.
Note that you will also use the devices evaluated here when you evaluate access control for connection destinations in the operation design.

If you decide to change the service template to be used after you have evaluated the services, re-evaluate the operation design and system design as necessary.

Related topics

- *Flow of Service Template Development* in the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*
- [3.4.4 Evaluating operations for access control by device](#)
- *Managing service templates* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.3.2 Evaluating the items to be considered when services are added

After you have decided the service template to be used, you evaluate the service names and category names, resource groups, and properties that are to be associated with the services as the items to be specified when services are added.

The following provides an overview of items that you must specify.

- Service names
Evaluate appropriate names for the services, based on their usage and operation.
- Category name
Evaluate classifying the services by category according to their usage and operation. Examples of categories for classifying services include target devices and execution timings.

You can facilitate management of services by classifying them into appropriate categories.

- Resource group

Evaluate assigning resource groups to the services based on the items evaluated in the operation design.

If you assign a resource group to a service, only the users who have the role for that resource group can manage and run that service.

If you do not create and use user-specific resource groups, use the built-in resource group (`All Resources`).

- Properties

The properties depend on the service template. Check the service template that you will be using, and then evaluate the property values to be specified. For details about the properties of service templates provided by JP1/AO, see the descriptions of the properties of individual service templates in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

If there is no need to change property values each time a service is run, evaluate specifying those properties when you add the service. If there are properties that will be shared among multiple services, evaluate defining them as shared service properties.

Some service templates display the properties specified by means of window operations when the service was added (or edited) so that you can change (overwrite) the property values when you run the service.

Related topics

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

3.3.3 Evaluating the items to be specified when services are run

You evaluate the items to be specified when services are run, including task names, properties, and execution timing.

- Task names

Evaluate suitable names for the tasks, as appropriate for the usage and operation of the services. The default service name is `service-name_YYYYMMDDhhmmss` (date and time the service was run).

- Properties

Evaluate the properties that are to be specified when a service is run. You must specify these properties each time the service is run. For details about the properties of service templates provided by JP1/AO, see the descriptions of the properties of individual service templates in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

- Execution timing

Evaluate when the services are to be run according to each service's operation and purpose.

The following table describes the available service execution timings.

Table 3–1: Service execution timings

Execution timing	Description
Now (immediate execution)	Runs the service immediately.
Later (date-and-time-specified execution)	Runs the service one time only on the date and at the time specified as the execution start date and time.
Recurring (periodic execution)	Runs the service at a specific interval (daily, weekly, monthly, or last day of the month) at the time specified as the scheduled start date and time.

Related topics

- *Submitting services for execution in the Job Management Partner 1/Automatic Operation Administration Guide*

3.3.4 Evaluating the shared service properties

You evaluate the values to be set for shared service properties, enabling appropriate property values to be shared among multiple services.

Shared service properties are classified into two types: The shared service properties that are defined in service templates, and the shared built-in service properties that are predefined in JP1/AO.

Shared service properties

Shared service properties can be added to a list in a window (**Service Share Properties** view) when a service template is imported. Such service properties will be deleted when the service template is deleted.

When you use service templates provided by JP1/AO (JP1/AO standard package and JP1/AO Content Set), note that the shared service property items and their initial values depend on the service template being used.

Check the shared service properties for the service template that you will be using and evaluate their input values.

Shared built-in service properties

For the shared built-in service properties, the items to be used in the JP1/AO system have already been defined and these items are used as common properties in JP1/AO. Evaluate the values for these properties according to the functions that you will be using.

Table 3–2: List of shared built-in service properties

Classification	Item	Description
Properties related to email notification	Enable/disable email notification function	Enables or disables the email notification function.
	SMTP server address	Specifies the SMTP server address.
	SMTP server port number	Specifies the port number of the SMTP server.
	SMTP server user ID	Specifies the user ID of the user who will be logging in to the SMTP server.
	SMTP server password	Specifies a password for the user who will be logging in to the SMTP server.
	Notification email sender	Specifies the sender of notification email.
	Notification email recipient (TO)	Specifies the recipient of notification email (TO).
	Notification email copy recipient (CC)	Specifies the recipient of a copy of notification email (CC).
	Notification email blind copy recipient (BCC)	Specifies the recipient of a blind copy of notification email (BCC).
Properties related to JP1/Base linkage	JP1 user name	Specifies the JP1 user name that will be running the service. This property is specified when JP1/AO is linked with JP1/Base. By default, the JP1 user name specified during installation is used.
	JP1 user password	Specifies a password for the JP1 user that will be running the service. This property is specified when JP1/AO is linked with JP1/Base. By default, the password specified during installation is used.
Property related to log information	Task's log output level	Specifies the task's log output level. Evaluate this item together with the error handling procedures.
Property related to public key authentication	Pass phrase of the private key (for SSH public key authentication)	Specifies a passphrase for a private key used for public key authentication.

Related topics

- [3.4.8 Evaluating the status notification method](#)

- *3.4.10 Evaluating error handling*
- *3.5.4 Evaluating the details of installation*
- *Setting shared service properties in the Job Management Partner 1/Automatic Operation Administration Guide*

3.4 Operation design

You evaluate how you will be running your JP1/AO system according to the service operations, including how to manage the target devices and users.

3.4.1 Evaluating users and access permissions

You need to evaluate the following as permissions appropriate for what a user does: User Management permissions, user groups, and roles.

You also evaluate the settings for user password conditions and locks. You can specify these settings in the security definition file (`security.conf`).

- **User Management permission**

Evaluate granting the `User Management` permission to the user account administrator who will manage users and user groups.

- **User groups**

Evaluate assigning user accounts to the appropriate user groups according to types and purposes of operation.

When you install JP1/AO, the user groups listed below are provided as built-in user groups. You can use these built-in user groups without creating your own user groups.

`AdminGroup`

The `Admin` role has been specified for the `All Resources` resource group.

`DevelopGroup`

The `Develop` role has been specified for the `All Resources` resource group.

`ModifyGroup`

The `Modify` role has been specified for the `All Resources` resource group.

`SubmitGroup`

The `Submit` role has been specified for the `All Resources` resource group.

- **Roles**

For each user group, evaluate specifying an appropriate role for accessing resource groups.

In JP1/AO, you can specify the functions to be made available to each user group by specifying the user group's role for resource groups.

Table 3–3: Roles and available functions

Role	Available function
Admin	<ul style="list-style-type: none">• Managing resource groups• Managing service templates• Developing service templates• Managing services• Running services
Develop	<ul style="list-style-type: none">• Managing service templates• Developing service templates• Managing services• Running services
Modify	<ul style="list-style-type: none">• Managing services

Role	Available function
Modify	<ul style="list-style-type: none"> Running services
Submit	<ul style="list-style-type: none"> Running services

Related topics

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

3.4.2 Evaluating operations using groups

A resource group is a group of services to which you want to restrict access. By allocating resource groups to user groups (groups of users classified by organization and job), you can control service access by user group. This enables you to efficiently manage the services according to the purposes of the user groups and to provide services as multi-tenant operations.

If you want to use the resource groups, you must evaluate the following items:

- Services to be registered in the resource groups
- Resource group names
- User groups allowed to access the resource groups

The resource groups evaluated here are allocated to services as described in *Evaluating the items to be considered when services are added* in the service design.

Related topics

- [2.2 Functions for managing operation targets](#)
- [3.3.2 Evaluating the items to be considered when services are added](#)
- [3.4.1 Evaluating users and access permissions](#)
- *Managing groups* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.4.3 Evaluating operations using external authentication linkage

External authentication linkage allows JP1/AO to link with JP1/Base or Active Directory.

- **Linking with JP1/Base**
If you wish to have JP1/AO use JP1 users managed by other JP1 products, consider using the JP1/Base authentication function for user management.
If you use the JP1/Base authentication function, there is no need to manage users or roles in JP1/AO.
- **Linking with Active Directory**
If you wish to have JP1/AO use Active Directory users and groups, consider linking with Active Directory for user management. This linkage can be used if JP1/AO uses Active Directory as an LDAP directory server.
When you link JP1/AO with Active Directory, you can select whether to link groups. In both cases, user authentication is performed by Active Directory.
 - If you do not link groups:

Users are registered to or deleted from user groups in JP1/AO.

Therefore, the same users registered in Active Directory must also be registered in JP1/AO. At this time, there is no need to set a password.

- If you link groups:

Groups in Active Directory are registered as JP1/AO user groups. At this time, users are registered to or deleted from user groups in Active Directory.

Therefore, there is no need to register a user in JP1/AO.

Related topics

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

3.4.4 Evaluating operations for access control by device

After you have determined the service template and the target devices (connection destinations) for services, evaluate basing access control on use of the management functions of the connection destinations. For details about the prerequisites for using the management functions of connection destinations, see [A.2 Prerequisites for connection destinations](#).

To restrict access to connection destinations, you must specify the IP address (or host name) for each connection destination, and register the resource groups that can access each connection destination. Therefore, you must evaluate the following items in advance.

Table 3–4: Settings in the connection destination definition

Classification	Item	Description
Connection destination information	Resource group of the services	Specify the name of a resource group to be associated with the connection destination. The services in the specified resource group can access only the specified connection destination. If <code>All Resources</code> is specified, the services in <code>All Resources</code> can access all connection destinations.
	Connection destination type	Select one of the following types: <ul style="list-style-type: none"> • Host name • IPv4 • IPv6
	Connection destination	Specify a connection destination appropriate for the selected connection destination type. You can specify a single connection destination, a range of connection destinations, or all connection destinations.
Authentication information ^{#1}	Protocol	Select one of the following authentication protocols according to the connection destination device: <ul style="list-style-type: none"> • Windows device: WMI • UNIX device: SSH (password authentication or public key authentication) • Other devices that support SSH or Telnet: SSH or Telnet

Classification	Item	Description
Authentication information ^{#1}	User ID ^{#2}	Specify the user ID of a user who can remotely log in to the host at the connection destination.
	Password ^{#2}	Specify the password for the user ID.
	Superuser password ^{#2}	If you selected SSH or Telnet as the protocol, specify the superuser password for the host at the connection destination.

#1

The authentication method depends on the definition of the plug-in. That is, authentication is performed based on the information specified in the plug-in property or based on the information in the connection destination definition. If authentication is performed based on the information specified in the plug-in property, authentication information in the connection destination definition is not used.

#2

Whether you need to specify a user ID, a password, and a superuser password depends on the type and setting of the plug-in. For details, see *List of definition parameters for connection destinations* in the *Job Management Partner 1/ Automatic Operation Administration Guide*.

Related topics

- *General command plug-in, File-forwarding plug-in, and Terminal connect plug-in* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*

3.4.5 Evaluating the work folders for target devices

When a file-forwarding plug-in or content plug-in runs on a UNIX device, a *work-folder* area is allocated on the target device, and then a file forwarded to the device is stored directly below the *work-folder* folder as shown below.

Figure 3–3: File forwarded to the target device (UNIX)

work-folder
└ File to be forwarded

The file is forwarded if either of the conditions shown below exists. The forwarded file is deleted when the plug-in terminates.

- A file-forwarding plug-in is used.
- A content plug-in with **Script** specified for Execution Mode is run.

If the OS of the target device is UNIX, the default *work-folder* is */tmp/Hitachi_AO*, which can be changed by the user.

To change the default *work-folder*, specify a new folder name in the `plugin.remoteCommand.workDirectory.ssh` key of the property file (`config_user.properties`).

However, if the OS of the target device is Windows, you cannot change the work folder, and the configuration of the work folder containing the files to be forwarded is also different. For details about the configuration of the work folder for the files to be forwarded in Windows, see *Files transferred to Windows systems* in the *Job Management Partner 1/ Automatic Operation Service Template Developer's Guide*.

Related topics

- *Procedure for setting scripts* in the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*
- *Property file (config_user.properties)* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

3.4.6 Evaluating port numbers used for target devices

You can change port numbers used to establish connections with target devices by running the following plug-ins:

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

To change the port number, specify a new port number in the connection-destination property file (connection-destination-name.properties) or property file (config_user.properties).

The setting in the connection-destination property file (connection-destination-name.properties) takes precedence over the setting in the property file (config_user.properties).

For details about the port numbers used by individual plug-ins by default, see the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

3.4.7 Evaluating the task retention period

You evaluate the retention period until a task whose processing has been completed is archived, the retention period until an archived task is deleted, and the retention period until a debug task is deleted.

Retention period until tasks are archived

A task whose processing has been completed is archived automatically from the list of tasks and displayed in the list of histories if either of the following conditions is satisfied:

- The specified retention period has expired.
- The specified maximum number of tasks has been reached.

If the number of tasks whose processing has been completed exceeds the specified maximum number of tasks, the excess tasks are archived automatically regardless of the specified retention period. Tasks whose retention period has expired are archived automatically even if the specified maximum number of tasks has not been reached.

Retention period until archived tasks are deleted

Among the tasks displayed in the list of histories, tasks that are in excess of the specified maximum number of tasks at the specified time are deleted automatically on a daily basis.

The service administrator must evaluate the following items, taking into account the task monitoring schedule:

- Period during which tasks whose processing has been completed are to be retained in the list of tasks
- Time at which tasks are to be archived automatically from the list of tasks, and time at which tasks are to be deleted automatically from the list of histories
- Maximum number of tasks to be retained in the list of tasks
- Maximum number of tasks to be retained in the list of histories

Retention period until debug tasks are deleted

A debug task generated during debugging is deleted without being archived if either of the following conditions is satisfied:

- The specified retention period has expired.
- The specified maximum number of tasks has been reached.

If the number of debug tasks whose processing has been completed exceeds the specified maximum number of tasks, the excess tasks are deleted automatically regardless of the specified retention period. Debug tasks whose retention period has expired are deleted automatically even if the specified maximum number of tasks has not been reached.

After you have installed JP1/AO, you use a property file (`config_user.properties`) to specify the items related to task retention.

Only tasks which have been executed are archived automatically. If you attempt to run a new service while the number of tasks exceeds the specified maximum number of tasks to be retained in the list of tasks, an error occurs and no task will be generated. Therefore, to ensure that new services can be run, you must first estimate the number of tasks to be executed daily, and then specify the maximum number of tasks to be retained in the list of tasks. However, this limitation does not apply to recurring tasks which have been executed.

Related topics

- *Managing Tasks* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.4.8 Evaluating the status notification method

You evaluate the method to be used to provide notification of system and task status.

JP1/AO monitors task status changes and the JP1/AO system's operating status and periodically issues JP1 events. If you link your JP1/AO with JP1/IM - Manager, you can check the issued JP1 events in a window of JP1/IM - View.

You can also set JP1/AO to send email notification to the service administrator when task errors and failures are detected.

The service administrator must consider the operation in evaluating the items listed below that are related to the notification method.

Table 3–5: Evaluation items related to the notification method

Notification method	Item	How to specify
JP1 event notification	Whether JP1 event notification is to be used	Property file (<code>config_user.properties</code>)
Email notification	Whether email notification is to be used	Shared built-in service properties
	SMTP server's IP address or host name	
	SMTP server's port number	
	User ID and password for logging in to SMTP server	
	Email sender (FROM)	
	Email recipients (TO, CC, BCC)	
	Number of retries and retry interval in the event of an email notification error	Property file (<code>config_user.properties</code>)
	Subject line and text message for email notification	Email notification definition file

Notification method	Item	How to specify
Email notification	Subject line and text message for email notification	Japanese environment: mailDefinition_ja.conf English environment: mailDefinition_en.conf Chinese environment: mailDefinition_zh.conf

After you install JP1/AO, you can specify the notification method items by using the property file (`config_user.properties`), the email notification definition file (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, or `mailDefinition_zh.conf`), or the shared built-in service properties in a window.

Related topics

- [3.3.2 Evaluating the items to be considered when services are added](#)
- *Property file (`config_user.properties`) and Email notification definition file (`mailDefinition_ja.conf`, `mailDefinition_en.conf`, or `mailDefinition_zh.conf`) in the *Job Management Partner 1/Automatic Operation Configuration Guide**

3.4.9 Evaluating maintenance

You make a plan for performing periodic maintenance of the operating environment after JP1/AO has been deployed. The following maintenance tasks are required in JP1/AO:

- **Backup**
Back up data periodically so you are prepared for failures and erroneous operations.
- **Database reorganization**
After a long period of operation, the database might become fragmented, adversely affecting processing speed. You use a command periodically to reorganize the database.

Related topics

- *Maintenance in the *Job Management Partner 1/Automatic Operation Administration Guide**

3.4.10 Evaluating error handling

If a failure occurred in JP1/AO, you can use a command (`hcmdsgetlogs`) to collect logs. The `hcmgetlogs` command collects a large amount of log information. Therefore, before you execute it, you must estimate the size needed for the logs and check the free disk space on the JP1/AO server. For details about the information that can be collected by using the `hcmgetlogs` command, see *hcmdsgetlogs (collecting log information)* in the manual *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*.

You should also check the items to be output to the logs and evaluate the size of the log files and their output level. After you have installed JP1/AO, you use a property file (`config_user.properties`) to specify the items to be output to logs.

You can use the shared built-in service properties to specify the output level of task logs that contain information, including the start and end of tasks and error information. For details about how to specify the output level of debug task logs, see the *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*.

Related topics

- [3.5.3 Checking the operating environment](#)
- *Troubleshooting JP1/AO* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.4.11 Evaluating audit logs

You evaluate audit logs, including whether audit logs are to be issued, the number of audit log files, and their file size.

.JP1/AO enables you to output audit logs that contain information about who performed operations, and when and what types of operations were performed.

The JP1/AO system administrator must evaluate the size and number of audit log files, taking into account the frequency and nature of audits. After you have installed JP1/AO, you use a property file (`config_user.properties`) to specify the size and number of audit log files.

Related topics

- *Outputting audit log entries* in the *Job Management Partner 1/Automatic Operation Administration Guide*

3.5 System design

You evaluate the type of system you want to configure based on the results of evaluating the operation design.

3.5.1 Evaluating the system configuration

You evaluate the appropriate system configuration according to the service templates and programs that you will be using.

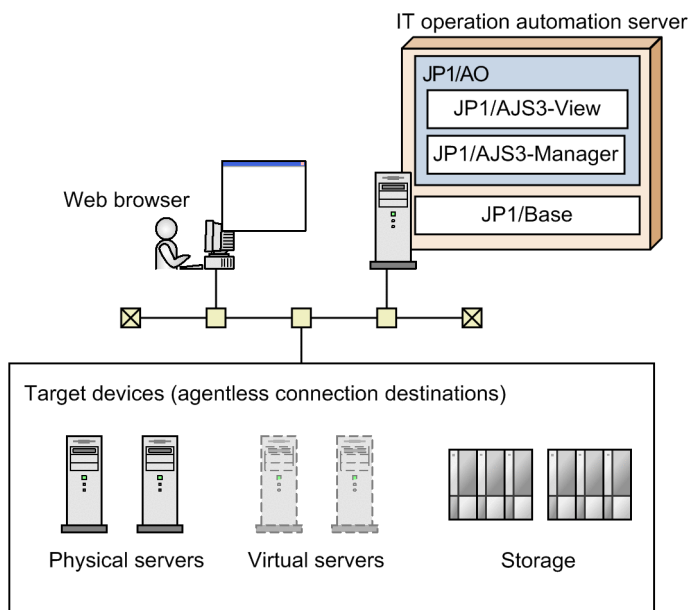
This subsection explains as examples of JP1/AO system configurations a basic system configuration, a cluster configuration, and a configuration linked with JP1/IM - Manager.

(1) Basic system configuration

This basic system configuration consists of an IT operation automation server, a Web browser for logging in to JP1/AO, and target devices (connection destinations) to which JP1/AO will connect.

JP1/AO's standard package also includes Common Component that provides a collection of functions available to all Hitachi Command Suite products. Common Component is installed as a part of JP1/AO and provides functions including user management, log output, and various commands.

Figure 3–4: Example configuration for a basic system



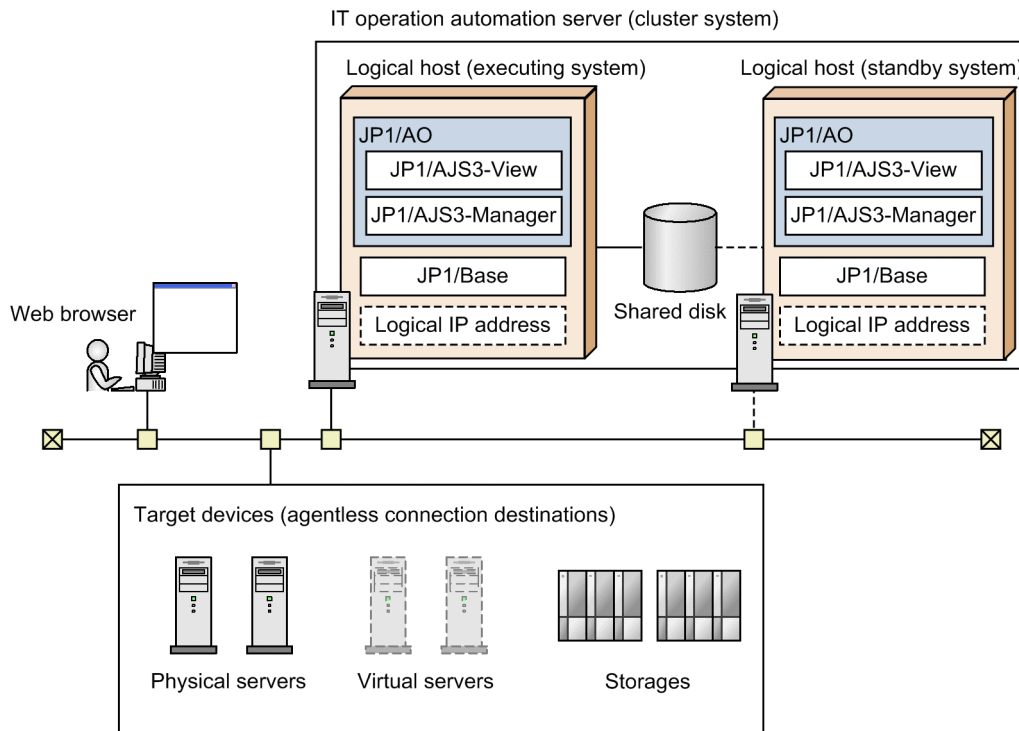
(2) Cluster configuration

JP1/AO supports operation in a cluster system. In a cluster system, if a failure occurs on the executing host that is running JP1/AO, operation can be continued by failing over to the standby host.

A host that is a unit of failover is called a *logical host*. A logical host name and a logical IP address are assigned to each logical host. The tasks in JP1/AO use the logical IP addresses stored on the shared disk for communications. When physical servers are swapped due to failover, information about the JP1/AO services, the shared disk, and the logical IP addresses is inherited by the standby host. For this reason, it appears to the users as if the server with the same IP address is still running.

Note that JP1/AO supports only the active-standby cluster configuration.

Figure 3–5: Example configuration for a cluster system



A JP1/AO cluster system has the following characteristics:

- The information stored on the shared disk includes JP1/AO's various definition files, log files, and the database used by Common Component.
- When window operations are used, the logical host name or logical IP address is used to connect to JP1/AO.

Related topics

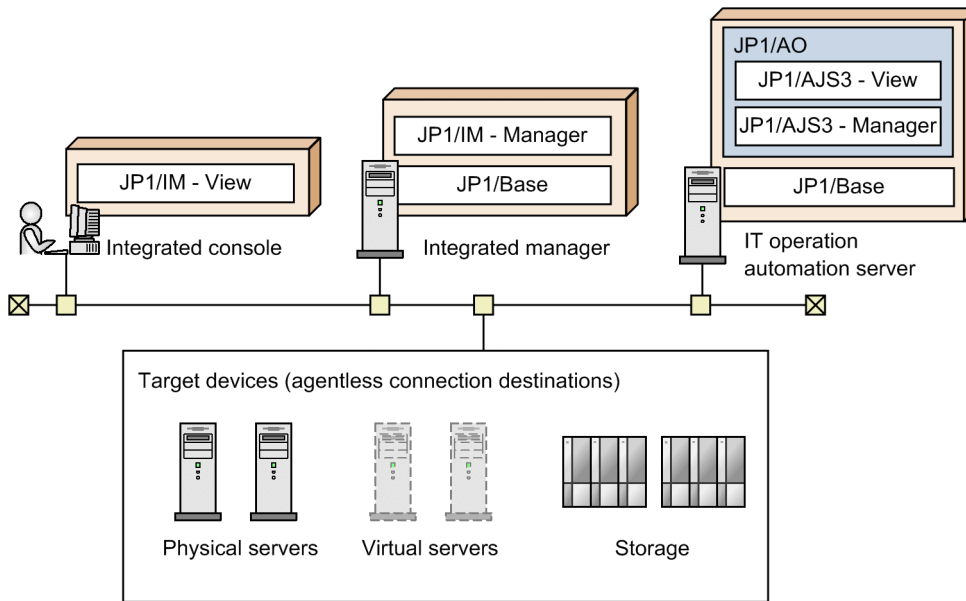
- *Setting up a cluster system* in the *Job Management Partner 1/Automatic Operation Configuration Guide*

(3) Configuration for linking with JP1/IM - Manager

You can monitor JP1 events centrally by linking your JP1/AO with JP1/IM - Manager.

To link JP1/AO with JP1/IM - Manager, JP1/Base on the IT operation automation server must be configured as a management target of JP1/IM - Manager.

Figure 3–6: Example configuration for linking with JP1/IM - Manager



To use single sign-on to log in to JP1/AO from the **Tool Launcher** window of JP1/IM - View, JP1/AO must be linked with the authentication function of JP1/Base.

Related topics

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

3.5.2 Evaluating the network settings

You can use HTTP or HTTPS as a communication protocol between JP1/AO servers and Web browsers. To use HTTPS, you need to acquire an SSL server certificate.

JP1/AO supports packet filtering firewalls and NAT (static mode) firewalls. To set up a firewall in the system, evaluate the settings so that the firewall permits JP1/AO communications.

You can change the default port number used by JP1/AO. If you change the default port number, make sure that the firewall permits communications using that port number.

Note that the port number used for communication between JP1/AO and target devices depends on the service template being used. For details about the port numbers used by JP1/AO-provided service templates for communication with target devices, see the descriptions of the properties of the individual service templates in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

Related topics

- [A.1 Lists of port numbers](#)
- *Connection-destination property file (connection-destination-name.properties), Procedure to enable HTTPS connections between Web browsers and JP1/AO, and Procedure to change the port number used for communications between JP1/AO and Web browsers in the Job Management Partner 1/Automatic Operation Configuration Guide*

3.5.3 Checking the operating environment

After you have determined the system configuration, check the following operating environment items for the JP1/AO server.

- Required OS
JP1/AO must be installed on one of the following OSs:
 - Windows Server 2008 R2 Standard
 - Windows Server 2008 R2 Enterprise
 - Windows Server 2008 R2 Datacenter
 - Windows Server 2012 Standard
 - Windows Server 2012 Datacenter
 - Windows Server 2012 R2 Standard
 - Windows Server 2012 R2 Datacenter
- Required software
To use JP1/AO, the following software is required:
 - JP1/Base 10-00 or later
- Memory and disk capacity requirements
See *Release Notes*.

You also need a Web browser to log in to the JP1/AO window. For details about the Web browsers supported by JP1/AO, see *Release Notes*.

3.5.4 Evaluating the details of installation

The items listed below are required when you install JP1/AO. Decide on these items according to the operating environment.

- User information
Specify the JP1 user name and password. You can also use a JP1/AO window operation to change the specified JP1 user information.
- Installation folder
The default is *system-drive*\Program Files (x86)\Hitachi\JP1AO.
- Database folder
The default is *system-drive*\Program Files (x86)\Hitachi\HiCommand\database\Automation.
- IP address or host name of the server on which JP1/AO is to be installed
The default is the host name of the server on which JP1/AO is installed.
- Port number of the server on which JP1/AO is to be installed
The default is 23015. The protocol used for communication with Web browsers is HTTP.

Related topics

- *New Installation* in the *Job Management Partner 1/Automatic Operation Configuration Guide*



Appendixes

A. Reference Information

This appendix provides information that will be helpful in using JP1/AO.

A.1 Lists of port numbers

This section provides lists of the port numbers to be specified and explains the firewall passage direction.

With some exceptions, the port numbers used in JP1/AO are set in the `services` file by default when the product is installed and the corresponding function is set up.

(1) Ports used for JP1/AO external connections

The following table lists the service names used for communication from JP1/AO to external systems and the default port numbers.

Table A–1: List of port numbers (for external connections)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartweb	22/tcp	JP1/AO ➡ Operation target	Y	Used for SSH communications by the following functions: <ul style="list-style-type: none">• Content plug-in (SSH connection)• General command plug-in (SSH connection)• File-forwarding plug-in (SSH connection)• Terminal connect plug-in (SSH connection)• Terminal command plug-in (SSH connection)• Terminal disconnect plug-in (SSH connection)
cjstartweb	23/tcp	JP1/AO ➡ Operation target	Y	Used for Telnet communications by the following functions: <ul style="list-style-type: none">• Terminal connect plug-in (Telnet connection)• Terminal command plug-in (Telnet connection)• Terminal disconnect plug-in (Telnet connection)
cjstartweb	445/tcp or 445/udp	JP1/AO ➡ Operation target	Y	Used for WMI communications by the following functions: <ul style="list-style-type: none">• Content plug-in (WMI connection)• General command plug-in (WMI connection)• File-forwarding plug-in (WMI connection)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartweb	135/tcp and 139/tcp	JP1/AO ➡ Operation target	Y	Used for WMI communications by the following functions: <ul style="list-style-type: none"> • Content plug-in (WMI connection) • General command plug-in (WMI connection) • File-forwarding plug-in (WMI connection)
cjstartweb	25/tcp ^{#1}	JP1/AO ➡ SMTP server	Y	Used for sending emails by the following functions: <ul style="list-style-type: none"> • Email Notification Plug-in • User-Response Wait Plug-in (when emails are sent to notify that the task is waiting for response) • Email notification function
httpsd	23015/tcp ^{#1}	Web browser ➡ JP1/AO	Y	Used to access HBase Storage Mgmt Web Service. Used for HTTP connection between a JP1/AO server and a Web browser.
httpsd	23016/tcp ^{#1}	Web browser ➡ JP1/AO	Y	Used to access HBase Storage Mgmt Web Service. Used for HTTPS connection between a JP1/AO server and a Web browser.
cjstartweb	359/tcp ^{#1}	JP1/AO ➡ LDAP directory server	N	Used to connect to an LDAP directory server for Active Directory linkage.
jp1ajs2qman	20241/tcp	JP1/AO ➡ JP1/AJS3 - Manager	N ^{#2}	Used to link with JP1/AJS3.
jp1ajs2qagt	20242/tcp	JP1/AJS3 - Manager ➡ JP1/AO	N ^{#2}	Used to link with JP1/AJS3.
jp1ajs2qnfy	20243/tcp	JP1/AO ➡ JP1/AJS3 - Manager	N ^{#2}	Used to link with JP1/AJS3.

Legend:

➡ : Unidirectional from left to right

↔ : Bidirectional from left to right and from right to left

#1

You can change this port number, if necessary. For details about the procedure, see Procedure to change the port number in the *Job Management Partner 1/Automatic Operation Configuration Guide*.

#2

If the service must be registered as an exception when JP1/AO is linking with JP1/AJS3, the user must register it manually.

(2) Ports used for JP1/AO internal connections

The following table lists the service names used for JP1/AO's internal communications and the default port numbers.

Table A–2: List of port numbers (for internal connections)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
jp1bsuser	20240/tcp	JP1/AO → JP1/Base	N	Used for communication with the user authentication server.
jp1ajs2report	20245/tcp	JP1/AO → JP1/AO	N	Used in the task-processing engine.
ajscdinetd	22250/tcp	JP1/AO → JP1/AO	N	Used in the task-processing engine.
cjstartweb	23031/tcp	JP1/AO → JP1/AO	N	Used to access the following services: <ul style="list-style-type: none"> • HBase Storage Mgmt Web SSO Service • Web server dedicated to HiCommand Single Sign On
jp1ajs2gw	23160/tcp	JP1/AO → JP1/AO	N	Used in the task-processing engine.
HiRDBEmbeddedEdition_JF1	23800/tcp	JP1/AO → JP1/AO	N	Used in an embedded database in a cluster configuration.

Legend:

→ : Unidirectional from left to right

↔ : Bidirectional from left to right and from right to left

A.2 Prerequisites for connection destinations

This section describes the prerequisites for connection destinations that can be used in JP1/AO.

For details about the OSs supported for connection destinations, see the *Release Notes*.

For details about the protocols that can be used for communication between JP1/AO servers and connection destinations, see *List of protocols used by each plug-in* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

For details about the OSs supported for the basic Plug-in, see *Operation target devices usable as connection destinations* in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

For details about the OSs supported for the service templates and plug-ins provided by JP1/AO, see the descriptions of the individual service templates and plug-ins in the manual *Job Management Partner 1/Automatic Operation Service Template Reference*.

When you use Windows as a connection destination, the following limitations apply to the users who can connect to the connection destination and to the administrative share setting.

(1) Users who can connect to the connection destination

The following Windows users are supported at the connection destination:

- Built-in Administrator^{#1}
- Users who belong to the Administrator group^{#1#2}
- Built-in Administrator of Active Directory^{#1}
- Users who belong to the Domain Admin group of Active Directory^{#1#2}

#1

This user cannot be promoted to administrator privileges when executing a command.

#2

If the OS of the connection destination meets one of the following conditions, specify the registry settings:

- The UAC function is enabled in Windows Server 2008.
- The UAC function is enabled in Windows Server 2008 R2.
- The OS is Windows Server 2012.
- The OS is Windows Server 2012 R2.

Table A–3: Registry settings (local user settings)

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Registry entry	LocalAccountTokenFilterPolicy
Value to be set in the registry entry	1 (DWORD)

Tip

You can also use the following command to set the registry values:

```
reg add HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1
```

(2) Administrative share setting

If you use a service template that uses one of the following plug-ins at the Windows connection destination, you must enable administrative shares:

- General command plug-in
- File-forwarding plug-in
- Content plug-in

To enable administrative shares, specify the registry settings shown in the following table, and then restart the OS at the connection destination.

Table A–4: Registry settings (administrative share setting)

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters
Registry entry	AutoShareServer
Value to be set in the registry entry	1 (DWORD)

Tip

You can also use the following command to set the registry values:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\parameters /v AutoShareServer /t REG_DWORD /d 1
```

Important note

System configurations in which multiple JP1/AO servers connect to a single Windows connection destination are not supported.

A.3 List of limit values of functions

The following table describes the limit values of the JP1/AO functions.

Table A–5: List of limit values of functions

Function	Item	Limit
Service management function	Number of plug-ins that can be added (total number of development plug-ins and release plug-ins, not including basic Plug-ins)	5,000
	Number of service templates that can be added (total number of development service templates and release service templates)	1,000
	Sum of the number of services that can be added in the Services window and the number of debug services that can be generated	1,000
	Number of category levels	10
Task management function	Number of tasks that can be managed (including debug tasks)	5,000
	Number of histories that can be managed	30,000
	Number of plug-ins that can be run concurrently	10
Connection destination management function	Number of connection destination definitions that can be created	10,000
	Number of successful authentication information items that can be saved	10,000
Service template editor function	Number of flow levels	25
	Number of steps per service template	320
	Number of steps per level	80

A.4 Version changes

(1) Changes in version 10-10

- A function for linking with JP1/AJS3 was added.
- A function for linking with JP1/IM - NP job contents was added to the functions for linking with other products.
- DevelopGroup was added as a built-in user group.
- The Develop role was added as a role that can be specified for a resource group.
- The Admin role can now be used to develop service templates.
- Telnet was added as a protocol that can be used.
- Email notification files now support Chinese environments in addition to the Japanese and English environments.
- The prerequisite OSs and software were added.
- The list of limit values of functions was added.

A.5 Reference material for this manual

This section provides reference information for this manual, including various conventions that are used.

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *Job Management Partner 1/Automatic Operation Overview and System Design Guide*^{#1} (3021-3-312(E))
- *Job Management Partner 1/Automatic Operation Configuration Guide*^{#1} (3021-3-313(E))
- *Job Management Partner 1/Automatic Operation Administration Guide*^{#1} (3021-3-314(E))
- *Job Management Partner 1/Automatic Operation Service Template Reference*^{#1} (3021-3-316(E))
- *Job Management Partner 1/Automatic Operation Messages*^{#1} (3021-3-317(E))
- *Job Management Partner 1/Automatic Operation Service Template Developer's Guide*^{#1} (3021-3-363(E))
- *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference*^{#1, #2} (3021-3-366(E))

#1: In the Job Management Partner 1/AO manuals, Job Management Partner 1/Automatic Operation is abbreviated to JP1/AO.

#2: For the manual issued in December 2014 or later, the title and reference number were changed from *Job Management Partner 1/Automatic Operation GUI and Command Reference* (3021-3-315(E)) to *Job Management Partner 1/Automatic Operation GUI, Command, and API Reference* (3021-3-366(E)).

- *Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3021-3-325(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3021-3-326(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3021-3-329(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3021-3-330(E))
- *Job Management Partner 1/Base User's Guide* (3021-3-301(E))
- *Job Management Partner 1/Base Messages* (3021-3-302(E))

Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
HDvM		Hitachi Device Manager
Hitachi Tuning Manager		Hitachi Tuning Manager Software
HP NNM or HP NNM-SE		HP Network Node Manager Software version 6 or earlier
		HP Network Node Manager Starter Edition Software version 7.5 or earlier
JP1/AJS3	JP1/AJS3 - Manager	Job Management Partner 1/Automatic Job Management System 3 - Manager
	JP1/AJS3 - View	Job Management Partner 1/Automatic Job Management System 3 - View
JP1/AJS3 - Agent		Job Management Partner 1/Automatic Job Management System 3 - Agent
JP1/Cm2/NNMi		Job Management Partner 1/Consolidated Management 2/Network Node Manager i
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
JP1/IM - NP		Job Management Partner 1/Integrated Management - Navigation Platform
JP1/IM - SS		Job Management Partner 1/Integrated Management - Service Support
JP1/PFM		Job Management Partner 1/Performance Management
JP1/PFM - Base		Job Management Partner 1/Performance Management - Base
JP1/PFM - Manager		Job Management Partner 1/Performance Management - Manager
JP1/PFM - RM		Job Management Partner 1/Performance Management - Remote Monitor for Microsoft(R) SQL Server
		Job Management Partner 1/Performance Management - Remote Monitor for Oracle
		Job Management Partner 1/Performance Management - Remote Monitor for Platform
JP1/PFM - WebConsole		Job Management Partner 1/Performance Management - Web Console
vCenter		VMware vCenter(TM) Server
VMware		VMware(R)
UNIX	HP-UX	HP-UX 11i V3 (IPF)
	Linux	Linux (R)
	Solaris	Solaris 10 (SPARC)
		Solaris 11 (SPARC)

Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
AIX	Advanced Interactive Executive
API	Application Programming Interface

Acronym	Full name or meaning
ASCII	American standard code for information interchange
BCC	Blind Carbon Copy
CA	Certificate Authority
CC	Carbon Copy
CD-ROM	Compact Disc Read Only Memory
CIFS	Common Internet File System
CPU	Central Processing Unit
CRLF	Carriage Return / Line Feed
CSR	Certificate Signing Request
CSV	Comma Separated Values
DAT	Digital Audio Tape
DB	Data Base
DN	Distinguished Name
DNS	Domain Name System
DP	Dual Processor
DWORD	Double Word
EUC	Extended UNIX Code
FC	Fibre Channel
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HQL	Hibernate Query Language
HSSO	HiCommand Single Sign-On
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
I/O	Input/Output
ICS	Internet Connection Sharing
ID	IDentifier
IE	Internet Explorer
IP	Internet Protocol
IPF	Itanium(R) Processor Family
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6

Acronym	Full name or meaning
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LUN	Logical Unit Number
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Information Center
NTP	Network Time Protocol
OS	Operating System
PC	Personal Computer
PCRE	Perl Compatible Regular Expressions
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
RDN	Relative Distinguished Name
RFC	Request For Comment
SAN	Storage Area Network
SCP	Secure Copy
SCSI	Small Computer System Interface
SHA	Secure Hashing Algorithm
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UAC	User Account Control
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VM	Virtual Machine
VMFS	Virtual Machine File System

Acronym	Full name or meaning
WMI	Windows Management Instrumentation
WSFC	Windows Server Failover Cluster
XML	Extensible Markup Language

Conventions: KB, MB, GB, and TB

This manual uses the following conventions: 1 KB (kilobyte) is 1,024 bytes. 1 MB (megabyte) is 1,024² bytes. 1 GB (gigabyte) is 1,024³ bytes. 1 TB (terabyte) is 1,024⁴ bytes.

B. Glossary

This glossary defines terms used in JP1/AO.

A

Admin role

One of the roles specified for resource groups. This role can manage resource groups, service templates, and services. It can also develop service templates and run services.

archive

In JP1/AO, archiving means moving tasks whose processing has been completed from the list of tasks to the list of histories. The detailed information is deleted from archived tasks .

B

build

To make a Development service template available for debugging and able to be added as a service in a development environment. A built Development service template is imported to a JP1/AO server.

built-in user group

A user group provided by JP1/AO. The following four built-in user groups are provided: AdminGroup, DevelopGroup, ModifyGroup, and SubmitGroup.

C

category

A categorization of services (such as by usage and type). Services are classified based on this information and managed in hierarchies.

cluster system

A system in which multiple servers are linked together and run as a single system, enabling applications to be run without interruption in the event of a failure. If a failure occurs on the server running applications (the active server), another server that has been on standby (a standby server) inherits the application processing. Inheriting processing in this manner is called failover. In general, this type of system is also called a node switching system because application processing is switched from the active node to the standby node.

Common Component

A component providing a collection of functions that can be used in all Hitachi Command Suite products. Common Component is installed as a part of JP1/AO and provides such functions as user management, log output, and various commands.

connection destination

The host at a connection destination that is managed by JP1/AO as a target of a service operation. Accesses from users to connection destinations can be restricted by associating the connection destinations with resource groups.

D

debugging

A series of operations for detecting problems of flows and plug-ins based on the results of a debug task, in order to verify operation of a Development service template.

debugger

A function provided by JP1/AO for supporting debugging of Development service templates.

debug service

A service that is generated and run when a Development service template is debugged. Unlike ordinary services, debug services need not be added in the **Add Service** dialog box or run in the **Submit Service** dialog box.

debug task

A task that is generated when a Development service template is debugged. This task is generated whenever a debug service is run. During debugging, problems of flows and plug-ins can be pointed out from the execution results of a debug task.

Develop role

One of the roles specified for resource groups. This role can manage service templates and services, can develop service templates, and can run services.

Development plug-in

A plug-in that is being created by the user, or a plug-in that was created by duplicating an existing plug-in. Development plug-ins are used in a development environment.

Development service template

A service template that is being created by the user, or a service template that was created by duplicating a Release service template. Development service templates are used in a development environment.

direct-access URL

A URL that displays a target dialog box immediately after login. The following three dialog boxes can be displayed: **Service Definition** dialog box, **Submit Service** dialog box, and **Task Details** dialog box.

E

external authentication linkage

A function for managing users by linking with JP1/Base's authentication function or Active Directory. Linking with JP1/Base's authentication function allows JP1/AO to use the JP1 user managed by other products. Linking with Active Directory allows the user to log in to JP1/AO by using Active Directory user information and use Active Directory to manage JP1/AO passwords.

F

flow

A flow of an automated procedure defined in a service template

H

history

An archived task whose processing has terminated.

Hitachi Command Suite

Product for providing centralized management of multiple storage systems, from configuration to monitoring of the storage environment, regardless of the platforms used.

Hitachi Tuning Manager

Product that provides the information needed to achieve central management of a network environment, including SAN.

J

job

A collection of commands, shell scripts, or Windows executable files.

jobnet

A collection of jobs that are related by their execution order. When a jobnet is executed, the jobs in the jobnet are executed automatically in the defined execution order.

JP1/AO Content Set

Product providing a package of multiple service templates. It provides a collection of templates that support a wide variety of types and fields of operations, including virtual server operations and cloud operations.

JP1/Automatic Operation

Product that provides functions needed to automate operation procedures and support run book automation.

JP1/Base

Product that provides functions fundamental to JP1/AO. Its functions include transmission of JP1 events and management of JP1 users. JP1/Base is a prerequisite software product for JP1/AO.

JP1/Cm2/NNMi

Product for achieving integrated network management, such as network configuration management, performance management, and failure management.

JP1 event

Information used by JP1 to manage an event that occurs in the system. The JP1 events are managed by JP1/Base's event service. JP1/Base records the JP1 events that occur in the system in a database.

JP1/Integrated Management

Product for centrally monitoring distributed systems. It enables the user to monitor the JP1 events that indicate job execution status and failures in distributed systems via the JP1/IM - View window.

JP1/Performance Management

Product for monitoring and analyzing issues related to system performance.

JP1 resource group

In JP1/Base (which is a required software product for JP1/AO), the management targets (resources), such as jobs, jobnets, and events, are classified into various groups. These groups of management targets (resources) are called JP1 resource groups.

JP1 user

A user managed by JP1/Base. Setting up an external authentication linkage with JP1/Base enables the JP1 users to log in to JP1/AO. The JP1 users are also the users of the task-processing engine.

L

layering step

A step that uses a flow plug-in. Using a layering step allows the user to create a layer of flows.

LDAP search user

A user who logs in to Active Directory to retrieve user information from an LDAP directory server. An Active Directory user who has permissions to access target user information can be specified as an LDAP search user.

M

Modify role

One of the roles specified for resource groups. This role can manage services and run services.

N

normal step

A step that uses normal plug-ins (that is, other than a flow plug-in and repeated execution plug-in). Using a normal step allows the user to perform processing defined in plug-ins.

P

plug-in

The minimum unit of processing for automated IT operations. Plug-ins include the JP1/AO standard-package plug-ins and JP1/AO Content Set Plug-ins. Of the JP1/AO standard-package plug-ins, plug-ins for general-purpose processing, such as email notification and repeated flow processing, are called basic Plug-ins.

plug-in icon file

An image file that can be set as a plug-in icon. Plug-in icons are displayed in a list of plug-ins and in the **Flow** view.

preset property

A definition of a property value based on the user's environment and operation that is specified in service templates. The preset properties enable the user to specify values appropriate to the user's environment and operation when services are added and edited. The preset properties can be specified in imported service templates.

profile

Data used for managing users, including the user IDs and addresses.

R

related line

A line that connects steps. An execution order of processing can be defined by deploying the steps required for a job and connecting them by using a related line.

release

To make a tested service template able to be added as a service in the product environment. A Development service template that has been released is called a Release service template, which cannot be edited. A released service template is imported to a JP1/AO server.

Release plug-in

A plug-in that was imported to JP1/AO by releasing a Development service template, or a plug-in included in the service templates provided by JP1/AO. Release plug-ins are used in the product environment.

Release service template

A Development service template that has been released is called a Release service template. The service templates provided by JP1/AO are also release service templates. Release service templates are used in the product environment.

repeated step

A step that uses a repeated execution plug-in. Using a repeated step allows a specified flow to be executed repeatedly.

resource group

A group of services and connection destinations.

resource group (cluster)

A group of clustered services that constitute a unit of service failover.

role

Role that restricts operations (such as managing and running services) for a given resource group. A role is set for each resource group. The four roles are the `Admin` role, the `Develop` role, the `Modify` role, and the `Submit` role.

S

service

In JP1/AO, an imported service template into which environment-specific property values are entered becomes what is called a service. Operation procedures are automated by running services.

service template

A template that enables various operation procedures for an IT system to be run by simply specifying property values and scheduling information from a JP1/AO window.

shared service property

A property whose value is shared among the services that run in JP1/AO. For example, if you define the host name, user name, and password for a server at the connection destination as shared service properties, you can skip entering these defined server information items each time you run a service. Shared service properties that are predefined by JP1/AO are called shared built-in service properties.

step

An element of a flow. One step executes one plug-in.

Submit role

One of the roles specified for resource groups. This role can run services.

T

task

The unit of processing that is generated by running a service. By checking the tasks, you can obtain the progress and results of automatic processing.

task monitor

A function that displays the progress of a selected task or debug task in flow format.

task-processing engine

An internal component of JP1/AO. It executes the flows contained in service templates.

U

user group

A group of users who use the same resource group and have the same permissions for that resource group.

User Management permission

Permission needed to manipulate all user accounts. A user with the `User Management` permission can use the functions for managing users and user groups.

Index

A

administrative share setting 55
Admin role (glossary) 62
archive (glossary) 62

B

build (glossary) 62
built-in user group (glossary) 62

C

category (glossary) 62
cluster system (glossary) 62
Common Component (glossary) 62
connection destination
 prerequisites 54
 users who can connect to 55
connection destination (glossary) 63

D

debugger (glossary) 63
debugging (glossary) 63
debug service (glossary) 63
debug task (glossary) 63
design procedure 32
development plug-in (glossary) 63
development service template (glossary) 63
Develop role (glossary) 63
direct-access URL (glossary) 63

E

external authentication linkage (glossary) 63

F

flow (glossary) 64
function
 for automating operation procedures 20
 for linking with other products 24
 for managing operation targets 22
 introduction to 19

G

glossary 62

H

history (glossary) 64
Hitachi Command Suite (glossary) 64
Hitachi Tuning Manager (glossary) 64

J

job (glossary) 64
jobnet (glossary) 64
JP1/AO
 benefit of deployment 13
 example application 15
 overview 11
JP1/AO Content Set (glossary) 64
JP1/AO system
 designing 29
 lifecycle 30
JP1/Automatic Operation (glossary) 64
JP1/Base (glossary) 64
JP1/Cm2/NNMi (glossary) 64
JP1/Integrated Management (glossary) 65
JP1/Performance Management (glossary) 65
JP1 event (glossary) 64
JP1 resource group (glossary) 65
JP1 user (glossary) 65

L

layering step (glossary) 65
LDAP search user (glossary) 65
list of limit values of functions 56

M

Modify role (glossary) 65

N

normal step (glossary) 65

O

operation design 39
 evaluating audit logs 46
 evaluating error handling 45
 evaluating maintenance 45
 evaluating operations for access control by device 41

- evaluating operations using external authentication linkage 40
- evaluating operations using groups 40
- evaluating port numbers used for target devices 43
- evaluating status notification method 44
- evaluating task retention period 43
- evaluating users and access permissions 39
- evaluating work folders for target devices 42
- operation design procedure 33
- operation procedure using JP1/AO 16

P

- plug-in (glossary) 65
- plug-in icon file (glossary) 66
- port
 - used for JP1/AO external connections 52
 - used for JP1/AO internal connections 54
- port numbers, list of 52
- preset property (glossary) 66
- profile (glossary) 66

R

- reference information 52
- related line (glossary) 66
- release (glossary) 66
- Release plug-in (glossary) 66
- release service template (glossary) 66
- repeated step (glossary) 66
- resource group (glossary) 66
 - cluster 66
- role (glossary) 66

S

- service (glossary) 67
- service design 35
 - evaluating items to be considered when services are added 35
 - evaluating items to be specified when services are run 36
 - evaluating service template to be used and targets of operation 35
 - evaluating shared service properties 37
- service design procedure 32
- service template (glossary) 67
- shared service property (glossary) 67
- step (glossary) 67
- Submit role (glossary) 67

- system design 47
 - checking operating environment 50
 - evaluating details of installation 50
 - evaluating network settings 49
 - evaluating system configuration 47
- system design procedure 34
- system operation, challenge faced by 12

T

- task (glossary) 67
- task monitor (glossary) 67
- task-processing engine (glossary) 67

U

- user group (glossary) 67
- User Management permission (glossary) 67