HITACHI
Inspire the Next

JP1 Version 12

JP1/Automatic Operation Overview and System Design Guide

3021-3-D02-40(E)

Notices

■ Relevant program products

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

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

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

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

■ Trademarks

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

* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License

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

* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

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

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

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

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

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

This product includes software developed by Andy Clark.

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

HITACHI
Inspire the Next

Hitachi, Ltd.

Java COMPATIBLE ENTERPRISE EDITION

Java COMPATIBLE

RSA SECURED

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

■ Issued

Mar. 2022: 3021-3-D02-40(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-D02-40(E)) and product changes related to this manual.

Changes	Location
Descriptions of the JP1/Base versions used for linking with other products were deleted.	2.4
Descriptions of the local execution function were changed.	3.4.5
Windows Server 2022 was added as a supported operating system.	3.4.6, 3.5.3
The following operating systems are now supported: • Red Hat Enterprise Linux 8 • Oracle Linux 8 • CentOS 8	3.5.3, A.4
Port numbers were added to or deleted from the description of the ports used for JP1/AO external connections. Also, comments were added.	A.1(1)
Descriptions related to Linux were deleted from the descriptions of port numbers and the direction of the firewalls used for JP1/AO internal connections.	A.1(2)
The conditions for which registry settings are required for administrative shares were changed.	A.2(2)
The description of the important item when connecting to one Windows agentless connection destination from multiple JP1/AO servers was changed.	A.2(2)

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

Preface

This manual provides an overview of the products and functions of JP1/Automatic Operation and explains the system design. In this manual, JP1/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
Active Directory		Microsoft(R) Active Directory
Windows Server 2008 R2		Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
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 2016	Windows Server 2016 Datacenter	Microsoft(R) Windows Server(R) 2016 Datacenter
	Windows Server 2016 Standard	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Windows Server 2019 Datacenter	Microsoft(R) Windows Server(R) 2019 Datacenter
	Windows Server 2019 Standard	Microsoft(R) Windows Server(R) 2019 Standard
Windows Server 2022	Windows Server 2022 Datacenter	Microsoft(R) Windows Server(R) 2022 Datacenter
	Windows Server 2022 Standard	Microsoft(R) Windows Server(R) 2022 Standard

Windows is often used generically to refer to Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Windows Server 2008 R2.

■ Formatting conventions used in this manual

This section describes the text formatting used in this manual.

Text formatting	Description
Character string	Italic characters indicate a variable.

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

■ Representation of JP1/AO-related installation folders

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

JP1/AO installation folder:

system-drive\Program Files\Hitachi\JP1AO

Common Component installation folder:

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

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

JP1/AO installation folder:

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

Common Component installation folder:

/opt/HiCommand/Base64

■ Diagrams of windows in the manual

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

Contents

Notices 2
Summary of amendments 8
Preface 9

1 Overview of JP1/AO 13
1.1 Challenges faced in system operations 14
1.2 Benefits of deployment 15
1.3 Example application of JP1/AO 17
1.3.1 Operation procedure using JP1/AO 18
1.4 User operations and approach to automation in JP1/AO 19

2 Introduction to functions 21
2.1 Functions for automating operation procedures 22
2.2 Functions for monitoring automated operation procedures 24
2.3 Functions for managing operation targets 25
2.4 Functions for linking with other products 27

3 Designing a JP1/AO system 32
3.1 JP1/AO system lifecycles 33
3.2 Design procedure 35
3.2.1 Service design procedure 36
3.2.2 Operation design procedure 36
3.2.3 System design procedure 37
3.3 Service design 38
3.3.1 Evaluating the operation procedure to be automated and the service template to be used 38
3.3.2 Evaluating the items to be considered when services are added 39
3.3.3 Evaluating the items to be specified when services are run 40
3.3.4 Evaluating the shared service properties 40
3.4 Operation design 42
3.4.1 Evaluating users and access permissions 42
3.4.2 Evaluating operations using groups 43
3.4.3 Evaluating operations using external authentication linkage 43
3.4.4 Evaluating operations for access control by device 44
3.4.5 Evaluating the method of executing plug-ins 45
3.4.6 Evaluating the working folders and execution directories for the operation-target devices 46
3.4.7 Evaluating port numbers used for target devices 47
3.4.8 Evaluating the task retention period 48

3.4.9 Evaluating the status notification method 49
3.4.10 Evaluating maintenance 50
3.4.11 Evaluating error handling 50
3.4.12 Evaluating audit logs 50
3.5 System design 52
3.5.1 Evaluating the system configuration 52
3.5.2 Evaluating the network settings 54
3.5.3 Checking the operating environment 55
3.5.4 Evaluating the details of installation 56

Appendix 57

A Reference Information 58
A.1 Lists of port numbers 58
A.2 Prerequisites for connection destinations 62
A.3 Version changes 64
A.4 Reference material for this manual 69

Glossary 74

Index 80

1 Overview of JP1/AO

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

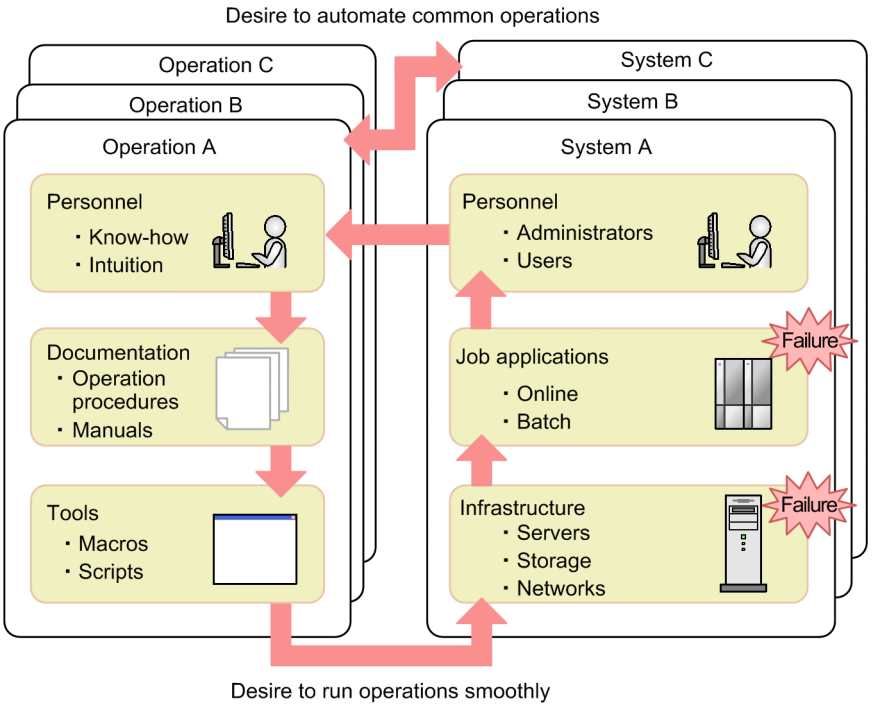
This chapter provides an overview of JP1/AO.

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

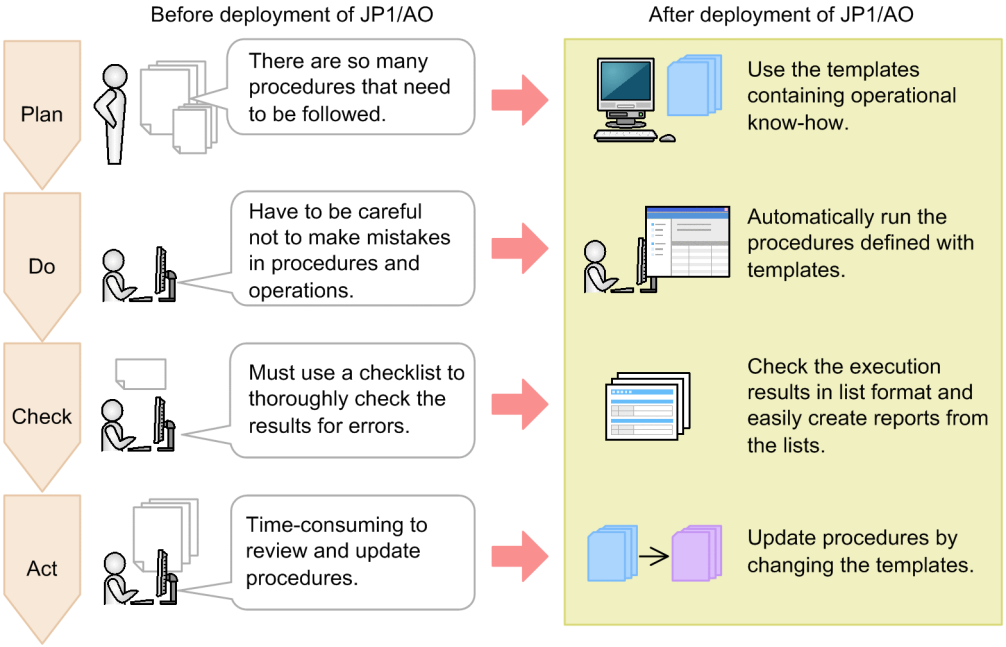
  In traditional system operations, the operators run multiple software programs by using multiple operation procedures. JP1/AO can reduce such labor-intensive tasks. JP1/AO can also reduce the incidence of human errors because it processes operation procedures automatically. This means that more time 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)

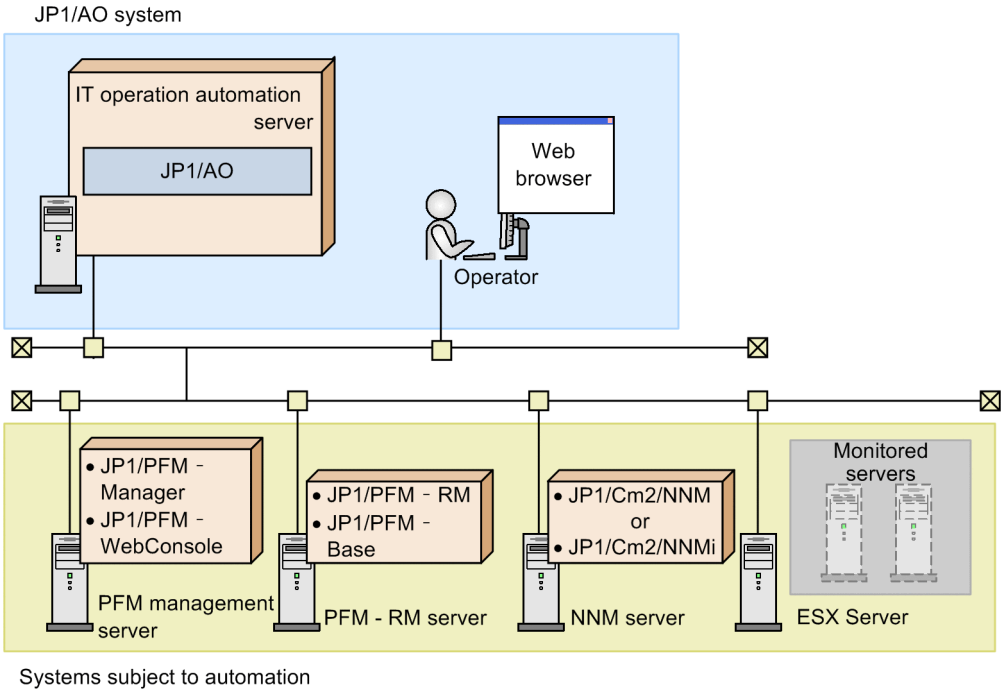
  Traditionally, the user must update the operation procedures each time the system configuration is changed.

  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.

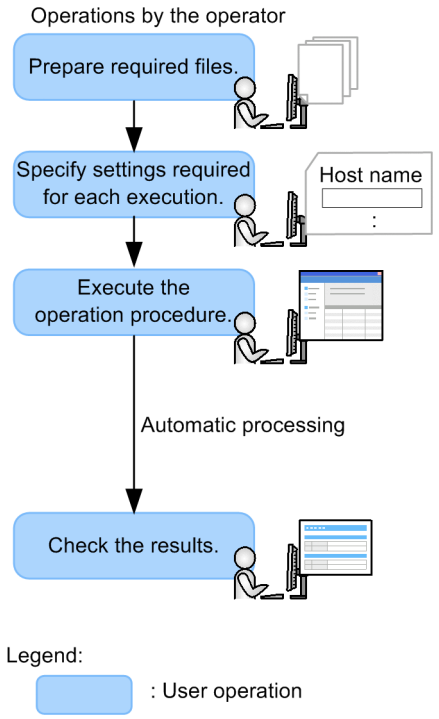
- Monitored servers

  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



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 the schedule type (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.

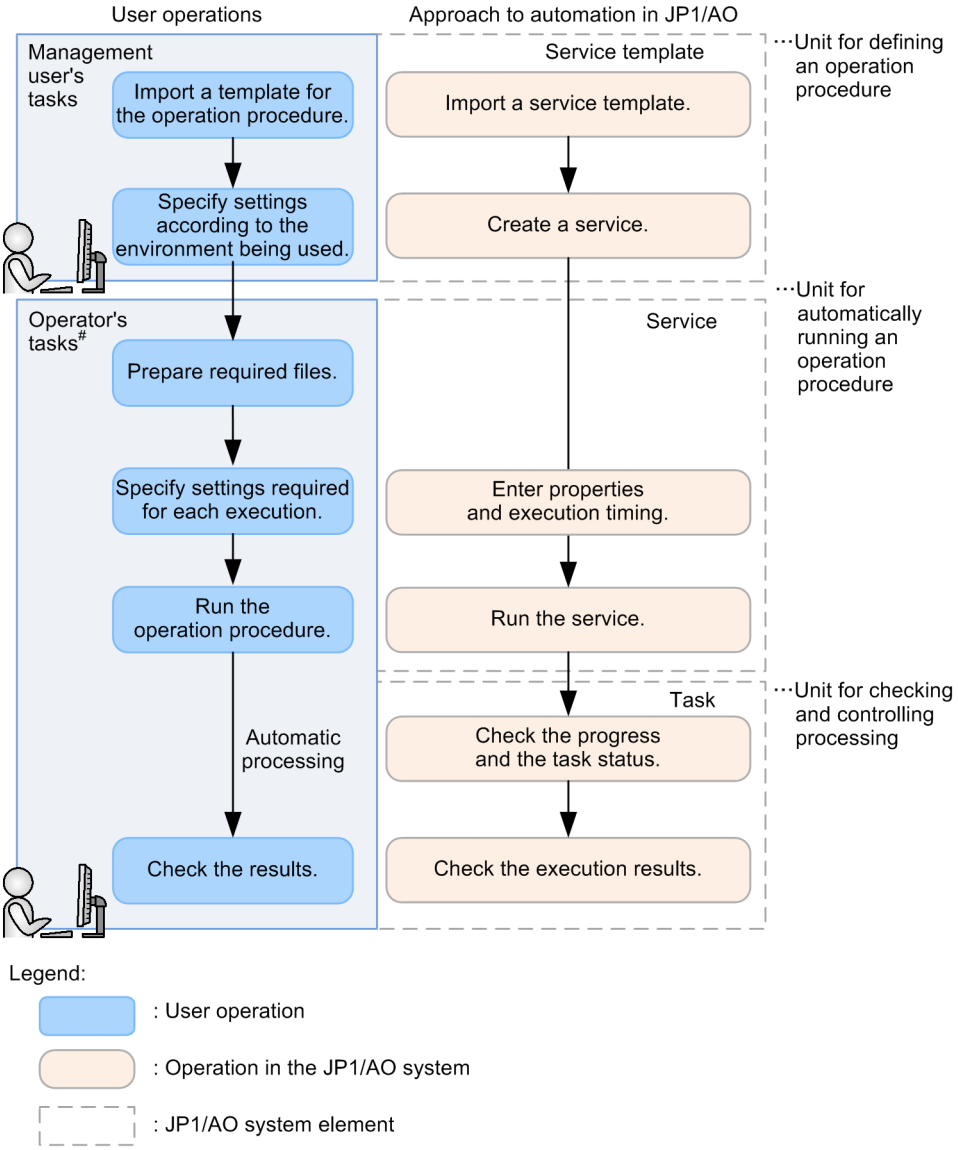
   If `Completed` is displayed in the JP1/AO window, automatic processing was successful.

   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 automation mechanism in JP1/AO



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. In the service template, enter information that is suitable for the environment to be applied (create a service).

   In the imported service template, enter information that is suitable for the environment, and create services. By using one service template, you can create 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 necessary information for each execution (enter properties and schedule type).

   You can specify information required for an operation procedure template by entering properties and a schedule type 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 topics

- 1.3.1 Operation procedure using JP1/AO

2 Introduction to functions

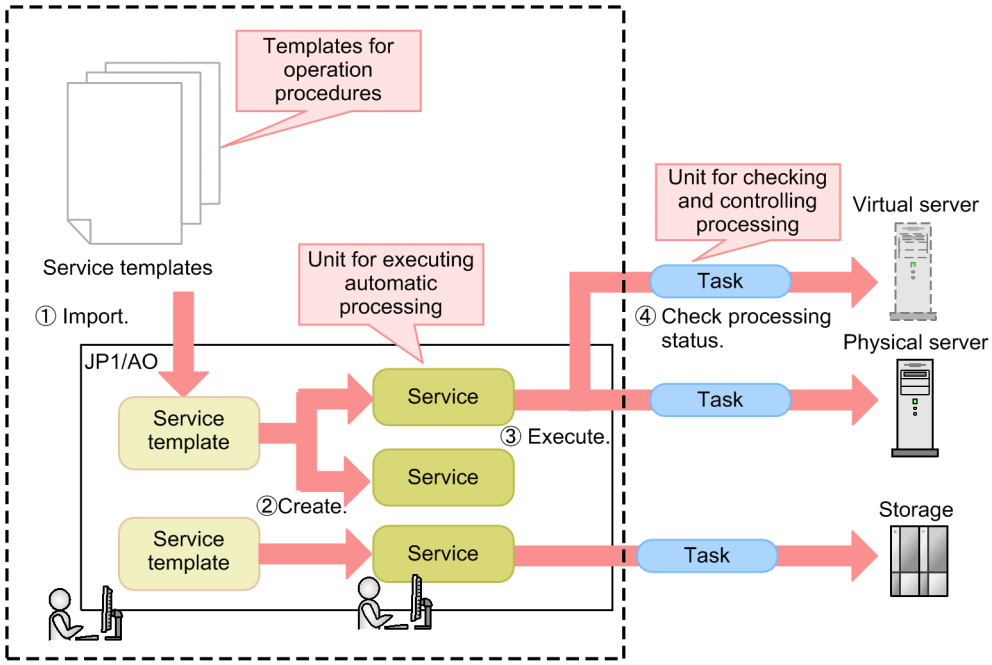
JP1/AO provides *functions for automating operation procedures* that enable you to define and perform automatic processing, and *functions for monitoring automated operation procedures* that enable you to check the execution status of automated processing. JP1/AO also provides *functions for managing 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 a direct access URL to display a target window. This chapter provides an introduction to these functions.

For details about the functions, see the *JP1/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: Flow of automating operation procedures



① Import a service template that defines an operation procedure.

② Enter information into the service template, and create a service.

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 Pack) are not supported. However, plug-ins provided by JP1/AO (JP1/AO standard package and JP1/AO Content Pack) that are called from such unsupported service templates are supported.

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

In the imported service template, enter information that is suitable for the environment, and create services. By using one service template, you can create multiple services suitable for different operation procedures and jobs.

Scheduling according to jobs - running services

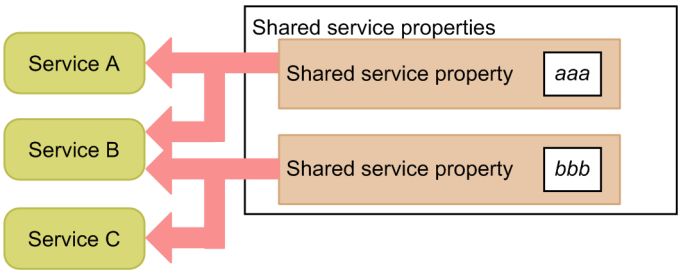
Enter information necessary for running a service and the schedule type, and then run the service. When a service is run, a task is generated and the automatic processing is started at the date and time that you have specified. You can specify (for the schedule type) immediate execution, repeated executions on a specified day of every week or at the end of each month, or execution of services on a certain date, at a certain time. Thus, you can plan a detailed schedule suitable for the users' jobs. This allows you to set a detailed schedule tailored to your business needs.

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



Categorizing and searching service templates and services, depending on the purpose (such as, for each job or for each division) - setting tags

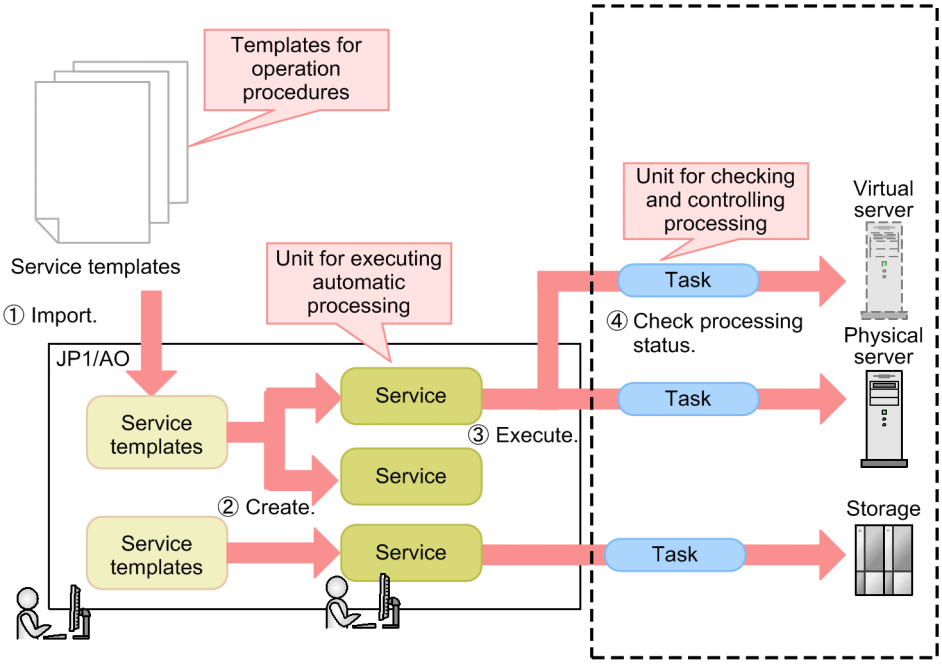
For a service template or service, you can set a tag that indicates the purpose or type of the template or service. You can also search service templates or services by using tags.

By setting multiple tags for one service, you can get a search result that is suitable for the condition (such as for each job or for each division).

2.2 Functions for monitoring automated operation procedures

This section provides an introduction to the principal functions needed to monitor automated operation procedures.

Figure 2-3: Flow of monitoring operation procedures



① Import (to JP1/AO) a service template that defines an operation procedure.

② Enter information into the service template, and create a service.

③ Enter information such as the execution timing, and then run the services.

④ Use the generated tasks to check the processing status.

Where statistics information of services and tasks can be checked - Dashboard

JP1/AO provides a Dashboard, which can be used to overview the statuses of services and tasks, to check at a glance whether there is any problem.

For services, information about services that frequently fail or that are frequently executed is displayed. Therefore, you can identify a problematic service at an early stage, and take action in advance to avoid a problem.

For tasks, the statuses of tasks that require users' actions and that are managed by login users are displayed. After you log in to JP1/AO, you can identify tasks that require users' actions by only checking a Dashboard.

By registering a frequently-executed service as a favorite, you can execute that service from a Dashboard.

Task list used to check the processing status and details windows used to check the progress for each step - managing tasks

JP1/AO provides the task list, which can be used to check at a glance the processing status. It also provides a details window, which can be used to check the progress of each step, or to output task logs. If you use a plug-in whose subsequent processing can be selected by the user according to the condition (user-response wait plug-in), you will be able to enter necessary information for a task that requires a user's decision during processing.

Searching for tasks by using tags - managing tags

A tag set for a service is inherited to the corresponding task. You can search for a task by using this tag.

2.3 Functions for managing operation targets

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

- Managing groups

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

- 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 service group, and centrally manage authentication information for hosts at connection destinations to reduce workload during operation.

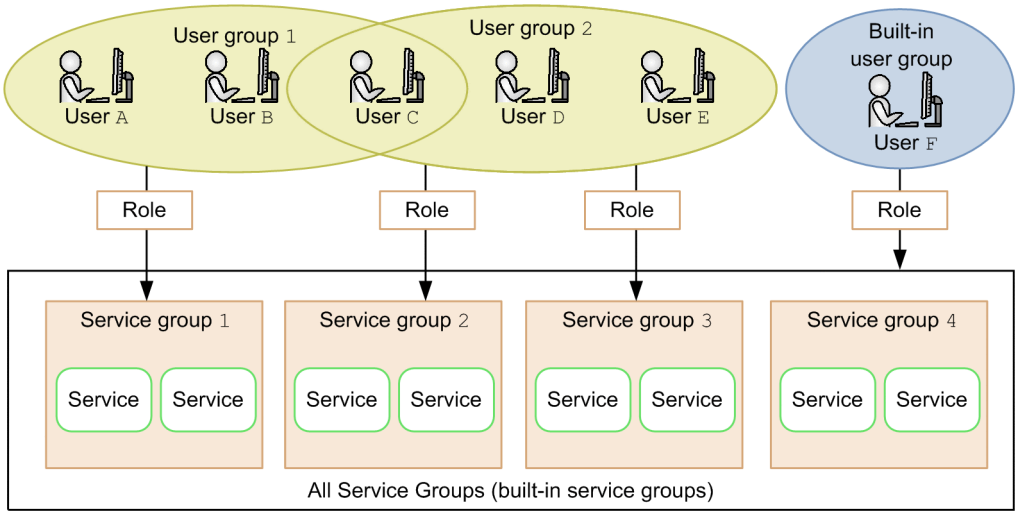
  Note that a host that is operated by command execution on a connection destination is not included in connection destinations.

Detailed access control according to operations and jobs - managing groups

By allocating service groups to user groups, you can restrict the services and tasks that each user can reference. 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 figure shows an example of access control using service groups and user groups.

Figure 2-4: Access control using service groups and user groups



In this example, users A, B, and C, who belong to user group 1, can use the services in service group 1. Users C, D, and E, who belong to user group 2, can use the services in service groups 2 and 3. User F, who belongs to the built-in user group, can access all services in JP1/AO because All Service Groups (built-in service groups) is assigned to the group.

Therefore, users A and B, who belong only to user group 1, cannot reference the services of service groups 2, 3, and 4.

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

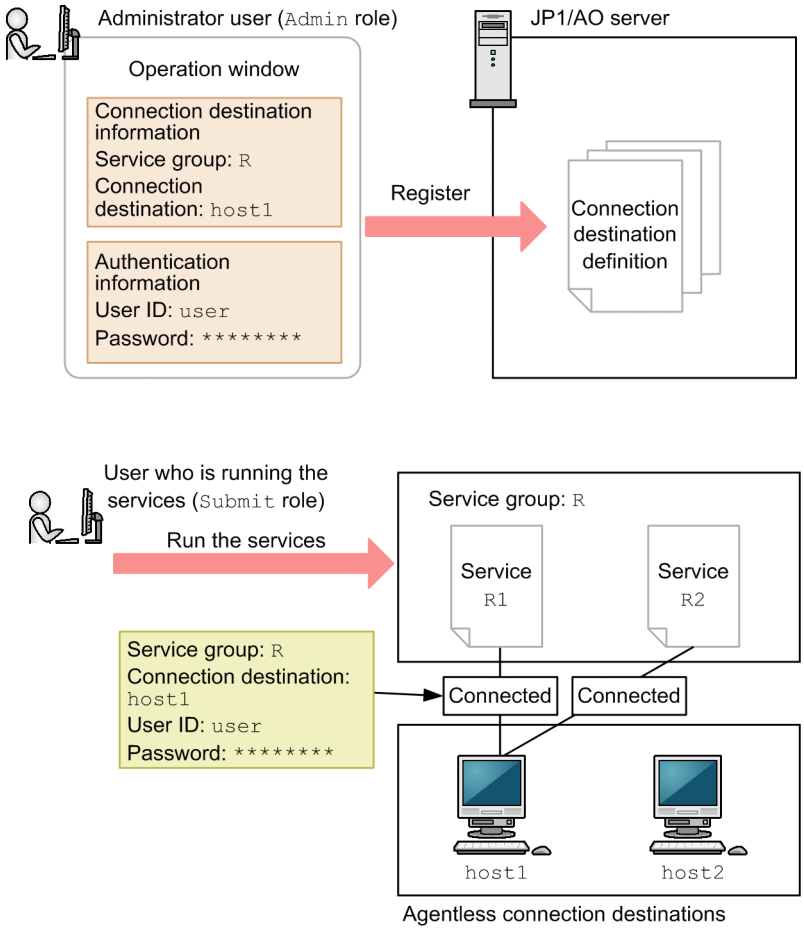
For example, if IT operations running at a data center are divided among multiple tenants, you can classify the services used by the individual tenants by service group and restrict the services that can be run by each user group. This allows you to prevent services of another tenant from being run by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

Agentless operations that reduce the management load - managing connection destinations

The function for managing the connection destination information (including service group names and host names) and the authentication information (including the user ID, password, and protocol that are 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 service 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 2-5: Example of agentless connection



In this figure, an administrator user with the Admin role uses window operations to register connection destination information and authentication information, and then a service execution user with the Submit role for service 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. Thus, by restricting connection-destination host for each service group, you can prevent services of another connection-destination host being run by mistake.

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.

2.4 Functions for linking with other products

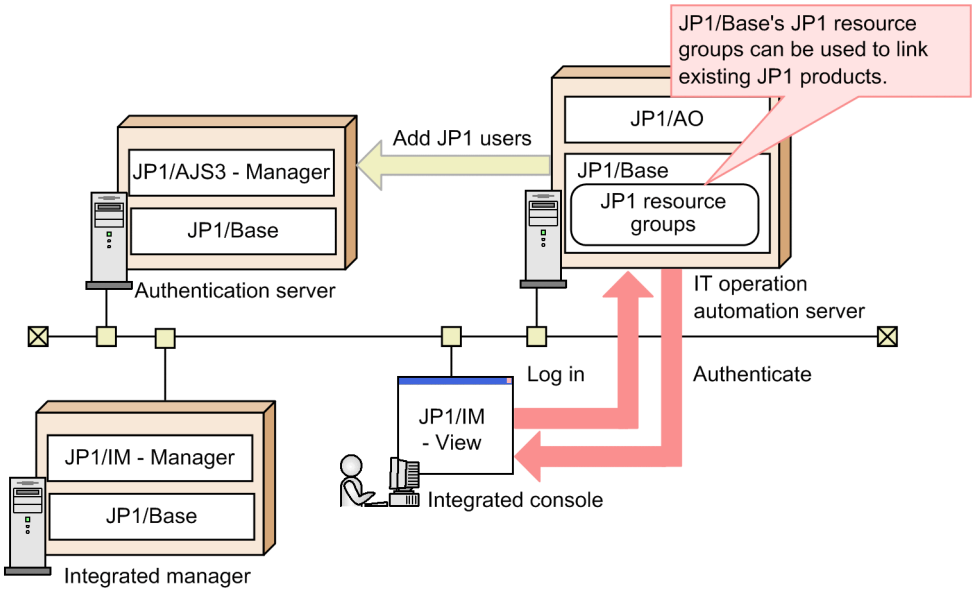
JP1/AO provides functions for improving the work efficiency of administrators, including email notifications when errors occur, a direct access URL that enables target windows to be displayed directly, and an API that calls JP1/AO functions from external programs.

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

JP1/AO enables you to use the authentication function of JP1/Base 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. The authentication server to be connected follows the definition of JP1/Base on the physical host. However SSL communication cannot be used to communication with an authentication server.

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 service group names and permissions in JP1/AO, you can manage those users as JP1/AO users.

Figure 2-6: 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.

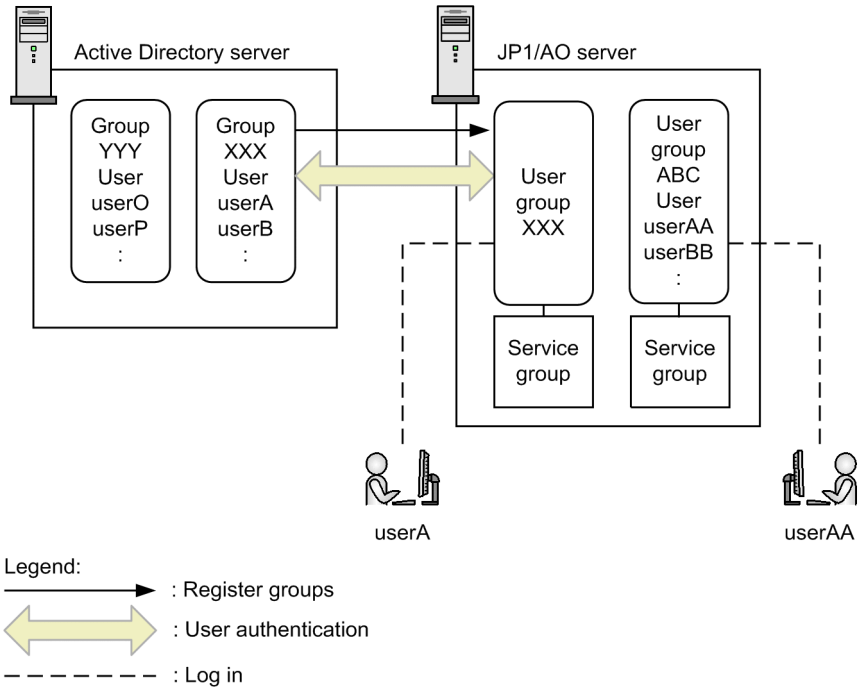
If you do not link groups, JP1/AO manages user groups and resources and Active Directory performs user authentication. You need to register the same users in both JP1/AO and Active Directory, but register passwords only in Active Directory.

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 2-7: Linkage with Active Directory (when linking groups)



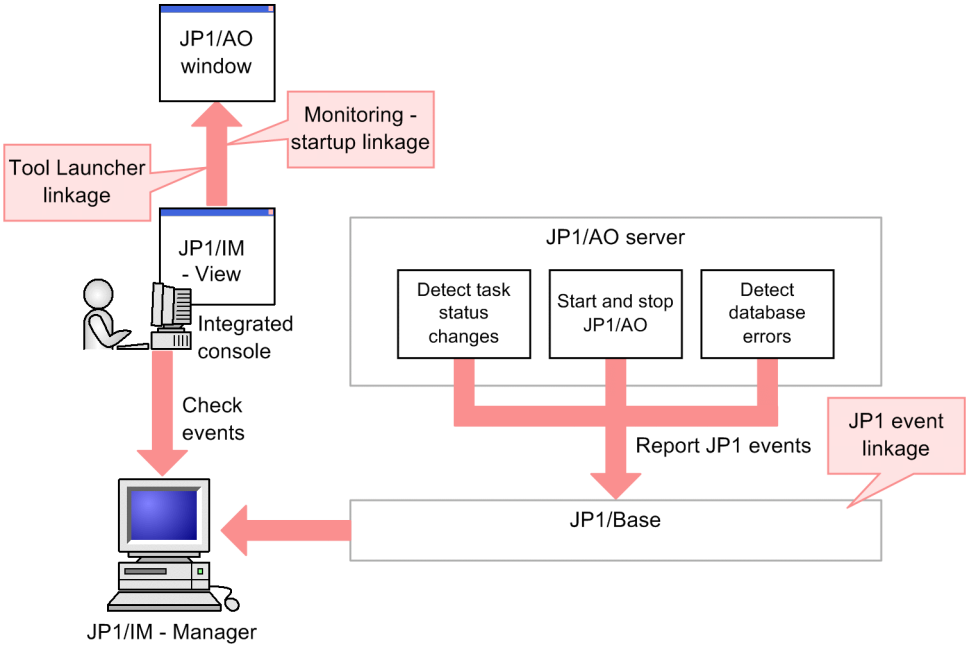
System monitoring linked with JP1/IM - linking with JP1/IM's event monitoring function

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

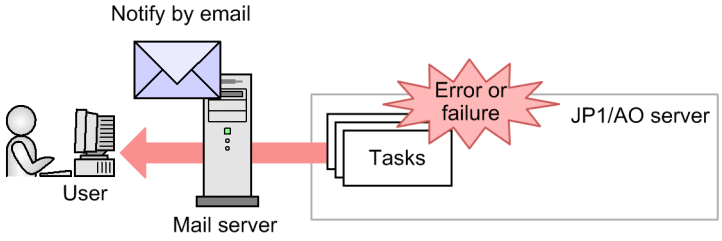
Figure 2-8: Linking with JP1/IM's event monitoring function



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

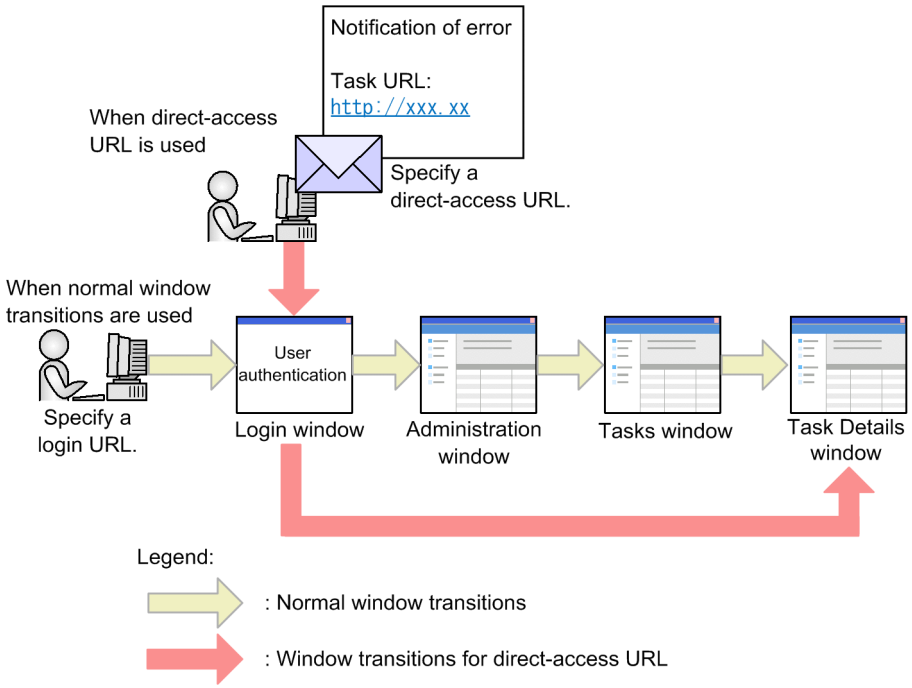


Improving work efficiency by directly accessing a target window - direct-access URL

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

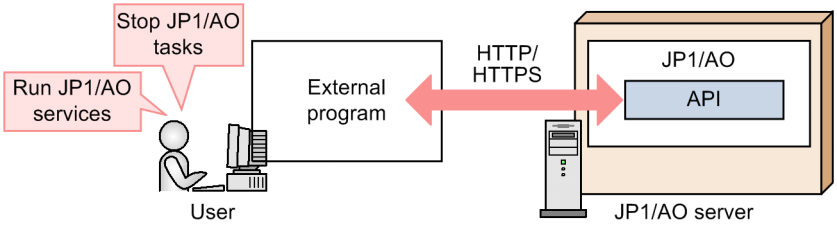
You can use the API to call JP1/AO functions from an external program. The API conforms to the REST (Representational State Transfer) architecture.

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 *JP1/Automatic Operation Command and API Reference*.

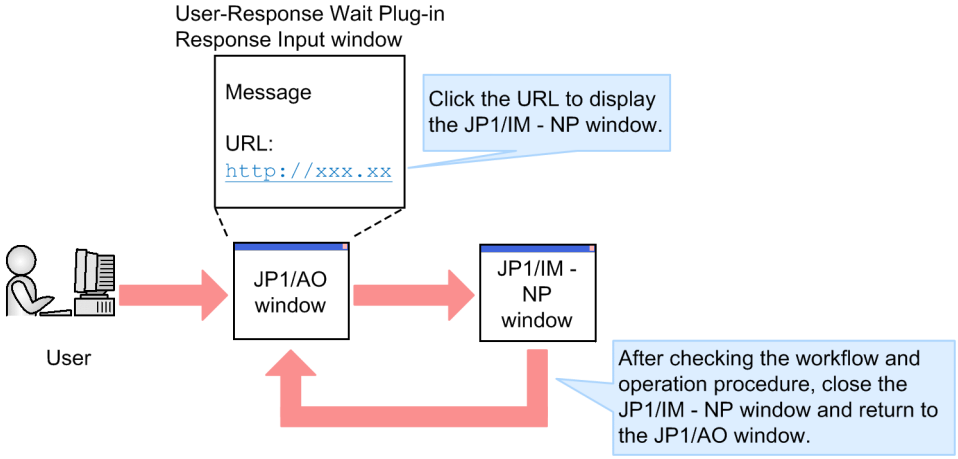
Figure 2-11: API



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 **Input Response** window, 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



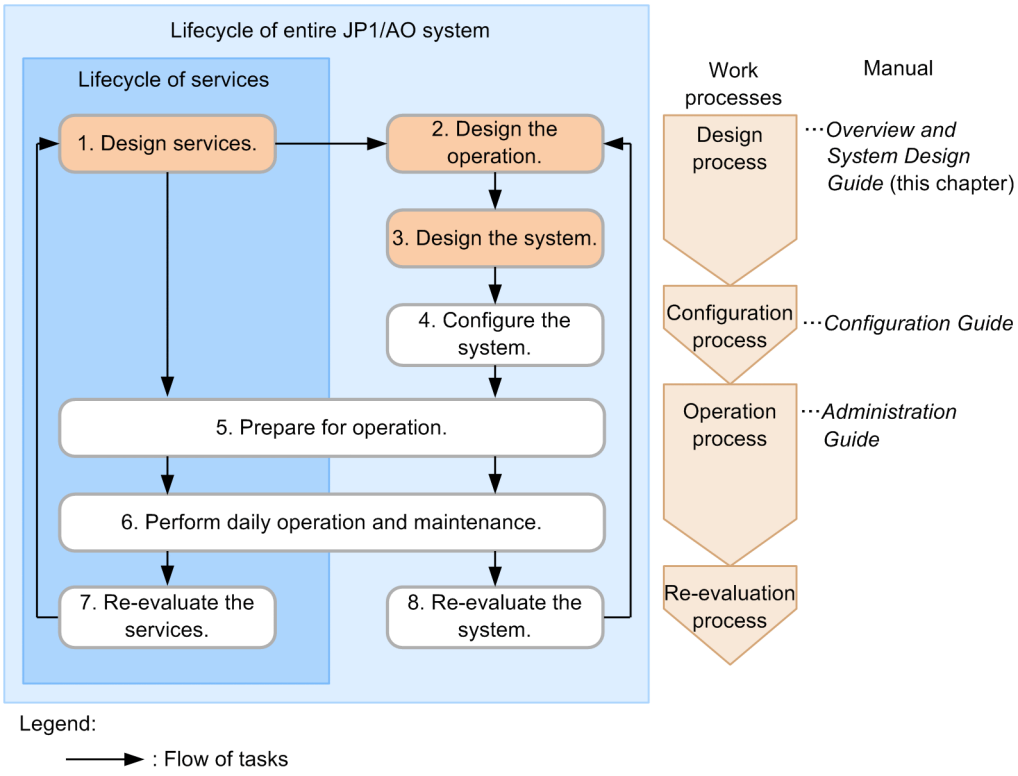
3 Designing a JP1/AO system

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 tag information).

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

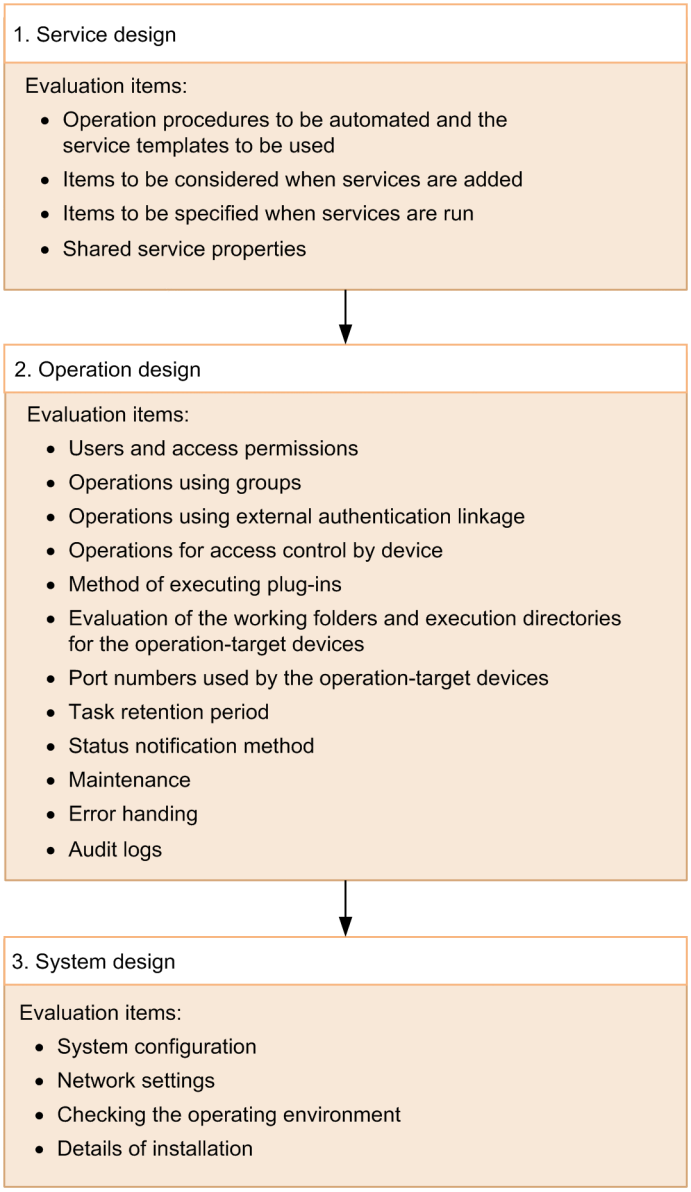
3.2 Design procedure

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 operation procedure to be automated and the service template to be used

   Evaluate and select the operation procedure to be automated and the service template that is suitable for your purpose. 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 tags 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 the schedule type 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 service groups so that accesses (by any user group) to services can be restricted.

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 method of executing plug-ins

   Evaluate the method of executing plug-ins when the operation-target host is the local host.

6. Evaluating the working folders and execution directories for the operation-target devices

   Evaluate the working folders and execution directories used when plug-ins are executed.

7. Evaluating the port numbers used by the operation-target devices

   Evaluate the port numbers used for connecting to the operation-target devices.

8. Evaluating the task retention period

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

9. 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.

10. Evaluating maintenance

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

11. Evaluating error handling

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

12. 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

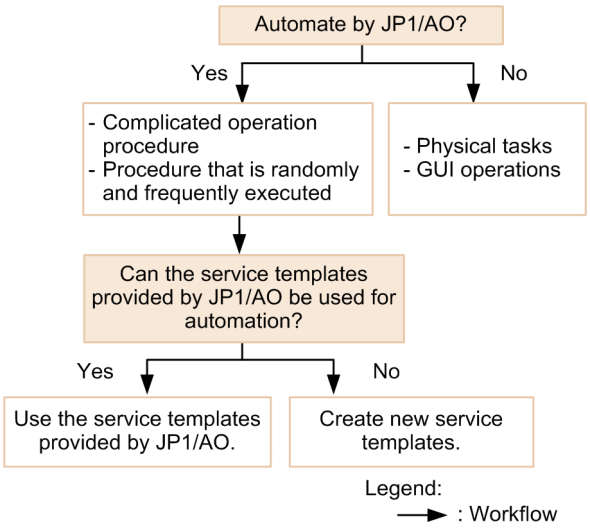
3.3 Service design

In the service design, identify the IT operations to be automated, and then evaluate the service templates to be used and the service running methods (including execution schedules and tag information).

3.3.1 Evaluating the operation procedure to be automated and the service template to be used

Evaluate the operation procedure to be automated by using JP1/AO. JP1/AO provides service templates in which information necessary for automating operation procedures is defined.

Figure 3-3: Evaluating the operation procedure to be automated and the service template to be used



When you automate the operation procedure by using JP1/AO, you can use various types of service templates in the JP1/AO standard package or JP1/AO Content Pack version. These service templates provided by JP1/AO support setup, operation, and error handling of various JP1 products, and virtual server and cloud operations.

Evaluate the following items, and decide the service template to use, to automate the operation procedure:

- Whether to use JP1/AO for automation

  Based on the procedure manual for the job you want to automate, consider the range of the operation procedure to be automated by the JP1/AO service template. Automation by JP1/AO is especially effective for complicated operation procedures and procedures that are randomly and frequently executed. All operations, except physical jobs and GUI operations, can be automated by JP1/AO.

- Whether the service templates provided by JP1/AO can support automation

  Check the detailed information about the service template, and evaluate whether to use the template. For details about service templates, see the descriptions of individual service templates in the manual *JP1/Automatic Operation Service Template Reference*. If you want to automate your system operations without using these JP1/AO-provided service templates, consider creating service templates and plug-ins. You can create a new service template or plug-in, or copy and edit a service template or plug-in that is provided by JP1/AO.

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 system. For details about the prerequisites for service templates, see the descriptions about the prerequisites for

individual service templates in the details windows of individual service templates, or in the manual *JP1/Automatic Operation Service Template Reference*.

The devices whose operation environment is verified here will be used during the process of evaluating operations for access control by device during 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 JP1/Automatic Operation Service Template Developer's Guide
- 3.4.4 Evaluating operations for access control by device
- Managing service templates in the JP1/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, evaluate the service names, and tags, service 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.

- Tags

  Evaluate appropriate tags to be set for the services. A tag is information for categorizing services, and is used as a key for searching. By categorizing services by using tag groups (large classification) and tags (small classification), you can easily search for the service you want. Decide the tags to be used for categorizing services, depending on the purpose of use and operation of services. For example, you can use tag groups for categorizing services by the operation-target devices or divisions, and tags for categorizing services by the purpose of operation or person in charge.

- Service groups

  Evaluate appropriate service groups to be assigned to the services, based on the evaluation result during operation design.

  If a service group is assigned to services, only the user groups that have a role for that service group can manage or execute the services.

  If you do not create and use your own service group, you can use the built-in service group (DefaultServiceGroup).

- 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 *JP1/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 JP1/Automatic Operation Administration Guide

3.3.3 Evaluating the items to be specified when services are run

You can evaluate the items to be specified when services are run, including task names, properties, and schedule type.

- 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 *JP1/Automatic Operation Service Template Reference*.

- Schedule type

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

  The following table describes the available schedule types for services.

  Table 3-1: Schedule types for services

Schedule type	Description
Immediate (immediate execution)	Runs the service immediately.
Schedule (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.
Recurrence (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

- Executing services in the JP1/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 are added to the list in the **Shared Properties Settings** area of the user interface when a service template is imported, and deleted when the service template is deleted.

When you use service templates provided by JP1/AO (JP1/AO standard package and JP1/AO Content Pack), 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 shared built-in service properties, the parameters used in the JP1/AO system are defined in advance, and used as common properties across the JP1/AO system. You can view shared built-in service properties in the **Shared Properties Settings** area and the **System Settings** area. Select the values to enter for these properties according to the functions you will be using.

Related topics

- 3.4.9 Evaluating the status notification method
- 3.4.11 Evaluating error handling
- 3.5.4 Evaluating the details of installation
- Setting Service Share Properties in the JP1/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 Service Groups service group.

  DevelopGroup

  The Develop role has been specified for the All Service Groups service group.

  ModifyGroup

  The Modify role has been specified for the All Service Groups service group.

  SubmitGroup

  The Submit role has been specified for the All Service Groups service group.

- Roles

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

  Table 3-2: Roles and available functions

Role	Available function
Admin	• Managing service groups • Managing service templates • Developing service templates • Managing services • Running services
Develop	• Managing service templates • Developing service templates • Managing services • Running services
Modify	• Managing services

Role	Available function
Modify	• Running services
Submit	• Running services

Related topics

- Managing Users in the JP1/Automatic Operation Administration Guide
- Security definition file (security.conf) in the JP1/Automatic Operation Configuration Guide

3.4.2 Evaluating operations using groups

Service group is a mechanism that classifies services into groups, each of which you want to restrict access to. By allocating service 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 service groups, you must evaluate the following items:

- Services to be registered in the service groups
- Service group names
- User groups allowed to access the service groups

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

Tip

Before creating a service group, you need to create a user group.

Related topics

- 2.3 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 JP1/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 JP1/Automatic Operation Administration Guide
- Linking to the JP1/Base authentication function in the JP1/Automatic Operation Configuration Guide
- Linking with Active Directory in the JP1/Automatic Operation Administration Guide
- Linking with Active Directory in the JP1/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 service groups that can access each connection destination. Therefore, you must evaluate the following items in advance.

Table 3-3: Settings in the connection destination definition

Classification	Item	Description
Connection destination information	Service group	Specify the name of a service group to be associated with the connection destination. The services in the specified service group can access only the specified connection destination. If `DefaultServiceGroup` is specified, the services in `DefaultServiceGroup` can access all connection destinations.
	Connection destination type	Select one of the following types: • 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.

Classification	Item	Description
Authentication information[#1]	Protocol	Select one of the following authentication protocols according to the connection destination device: • Windows device: `Windows`[#2] • UNIX device: `SSH` (password authentication, public key authentication, or keyboard interactive authentication) • Other devices that support `SSH` or Telnet: SSH or Telnet
	User ID[#3]	Specify the user ID of a user who can remotely log in to the host at the connection destination.
	Password[#3]	Specify the password for the user ID.
	Superuser password[#3]	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

If you select `Windows`, SMB and WMI are used.

#3

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 *Information set in definitions of Connection Destinations* in the *JP1/Automatic Operation Administration Guide*.

Related topics

- General command plug-in, File-transfer plug-in, and Terminal connect plug-in in the manual JP1/Automatic Operation Service Template Reference

3.4.5 Evaluating the method of executing plug-ins

You need to evaluate the method of executing plug-ins when the operation-target host is the local host[#].

If the operation-target host is the local host, you can use the following plug-ins to directly start the process and execute a command, or to copy files:

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

This function is called *local execution function*.

You can specify whether to enable the local execution function by using the key `plugin.localMode` in the user-specified properties file (`config_user.properties`) after JP1/AO is installed.

The following table lists and describes the items whose functions are different when the local execution function is enabled and disabled.

Table 3-4: Difference between the functions when the local execution function is enabled and disabled

Items whose functions are different when the local execution function is enabled and disabled	Local execution function	
	Enabled	Disabled
Execution user of a plug-in	Differs depending on the OS on the local host. In Windows System account In Linux root user	User connecting to the operation-target device
How connection destinations are treated	The definition of the local host is unnecessary.	The connection destination is authenticated according to the connection destination and authentication information.

Tip

If you enable the local execution function, authentication for agentless connection is omitted, so you can reduce resource consumption.

#

The operation-target host of a plug-in is judged as the local host in a certain condition. This condition is that either of the following IP addresses is the same as the loopback address or the IP address that is set on the local host and can be connected from an external device:

- IP address specified for the operation-target host of the plug-in (on a cluster system, physical IP address or logical IP address of the active server)
- IP address resolved from the host name specified for the operation-target host of the plug-in (on a cluster system, physical host name or logical host name of the active server)

Related topics

- General command plug-in and File-transfer plug-in in the manual JP1/Automatic Operation Service Template Reference
- User-specified properties file (config_user.properties) in the JP1/Automatic Operation Configuration Guide
- Reserved plug-in properties for specifying execution-target hosts and authentication information in the JP1/Automatic Operation Service Template Developer's Guide
- Information set in definitions of Connection Destinations in the JP1/Automatic Operation Administration Guide

3.4.6 Evaluating the working folders and execution directories for the operation-target devices

You need to evaluate the working folders and execution directories that are used when a plug-in is executed.

When the OS on the operation-target device is Windows

You can change the default execution directory used when a content plug-in is executed, to any directory you want. Specify the execution directory in the connection-destination property file (*connection-destination-name*`.properties`) or user-specified properties file (`config_user.properties`).

You can also change the working folder used when a general command plug-in, File-transfer plug-in, or content plug-in (when Execution Method is Script) is executed, to any directory you want. Specify the working folder in the connection-destination property file (*connection-destination-name*`.properties`).

However, note the following when you specify the working folders and execution directories:

- The execution directories and working folders must be placed on the same drive.
- If the OS on the operation-target device is Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022 in a cluster environment, you must specify the working folders.
- If you execute a script for a content plug-in when the OS on the operation-target device is Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022 in a cluster environment, you must specify the execution directory.

When the OS on the operation-target device is UNIX

You can change the execution directory when a content plug-in is executed, to any directory you want. Specify the execution directory in the connection-destination property file (*connection-destination-name*`.properties`) or user-specified properties file (`config_user.properties`).

If you execute a File-transfer plug-in or content plug-in (when Execution Method is Script), the working folder is created. You can change the working folder to any directory you want, in the connection-destination property file (*connection-destination-name*`.properties`)

Related topics

- Method for specifying scripts, Files transferred to Windows systems, and Files transferred to UNIX systems in the JP1/Automatic Operation Service Template Developer's Guide
- Connection-destination property file (connection-destination-name.properties) and User-specified properties file (config_user.properties) in the JP1/Automatic Operation Configuration Guide

3.4.7 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-transfer 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 user-specified properties file (`config_user.properties`).

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

For details about the port numbers used by individual plug-ins by default, see the manual *JP1/Automatic Operation Service Template Reference*.

3.4.8 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 user-specified properties 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 JP1/Automatic Operation Administration Guide

3.4.9 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	user-specified properties file (`config_user.properties`)
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 reties and retry interval in the event of an email notification error	user-specified properties file (`config_user.properties`)

	Subject line and text message for email notification	Email notification definition file
		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 user-specified properties 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
- User-specified properties file (config_user.properties) and Email notification definition file (mailDefinition_ja.conf, mailDefinition_en.conf, or mailDefinition_zh.conf) in the JP1/Automatic Operation Configuration Guide

3.4.10 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 JP1/Automatic Operation Administration Guide

3.4.11 Evaluating error handling

If a failure occurred in JP1/AO, you can use a command (`hcmds64getlogs`) to collect logs. The `hcmds64getlogs` 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 `hcmds64getlogs` command, see *hcmds64getlogs (collecting log information)* in the manual *JP1/Automatic Operation Command and API Reference*.

After you have installed JP1/AO, you can set the size and number of log files in the user-specified properties file (`config_user.properties`).

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 *JP1/Automatic Operation Service Template Developer's Guide*.

Related topics

- 3.5.3 Checking the operating environment
- Troubleshooting during system operation in the JP1/Automatic Operation Administration Guide

3.4.12 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 user-specified properties file (`config_user.properties`) to specify the size and number of audit log files.

Related topics

- Outputting audit log data in the JP1/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.

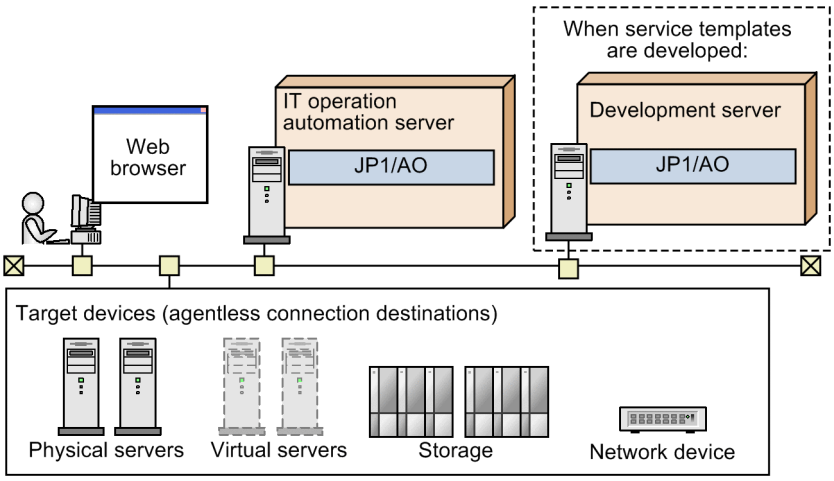
This subsection explains as examples of JP1/AO system configurations a basic system configuration, a cluster configuration, and a configuration linked with JP1/IM - Manager.

(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



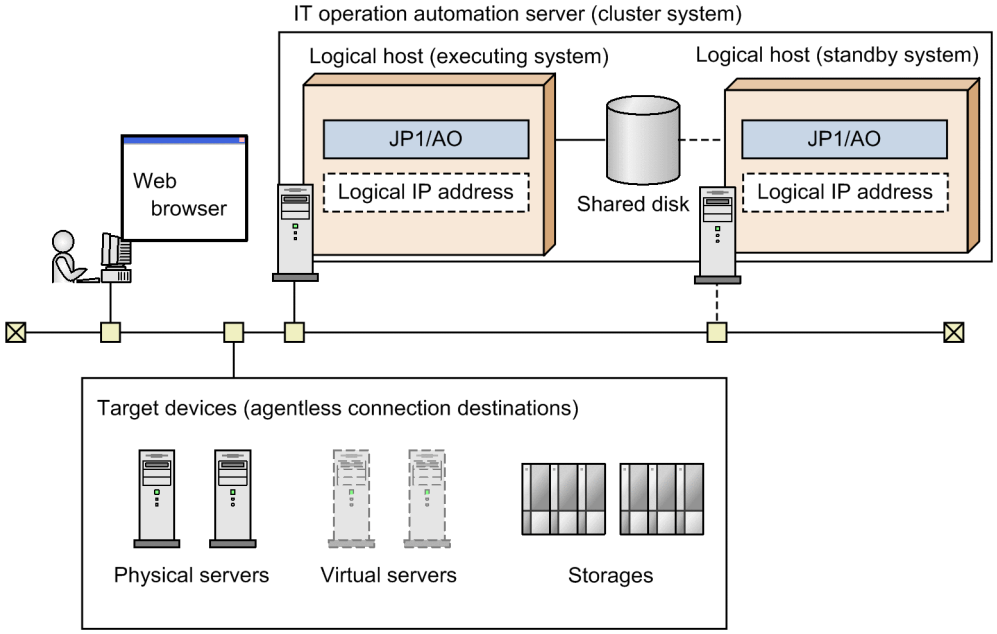
(2) Cluster configuration

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

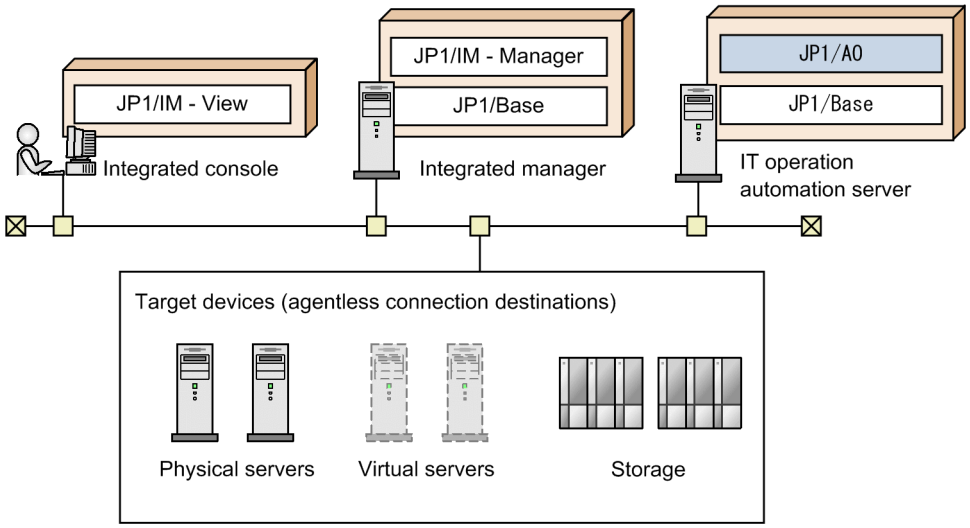
- Setting up a cluster system in the JP1/Automatic Operation Configuration Guide

(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, on the IT operation automation server, JP1/Base must be configured to be managed by 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 JP1/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 *JP1/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 JP1/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
  - Windows Server 2012 Standard
  - Windows Server 2012 Datacenter
  - Windows Server 2012 R2 Standard
  - Windows Server 2012 R2 Datacenter
  - Windows Server 2016 Standard
  - Windows Server 2016 Datacenter
  - Windows Server 2019 Standard
  - Windows Server 2019 Datacenter
  - Windows Server 2022 Standard
  - Windows Server 2022 Datacenter
- Linux
  - Red Hat Enterprise Linux 6 (x64)
  - Red Hat Enterprise Linux 7
  - Red Hat Enterprise Linux 8
  - Oracle Linux 6 (x64)
  - Oracle Linux 7
  - Oracle Linux 8
  - CentOS 6 (x64)
  - CentOS 7
  - CentOS 8
  - SUSE Linux 12

For details about the required OS and latest information, see *Release Notes*.

Required software

You 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*.

Memory and disk capacity requirements

See *Release Notes*.

Required service

If the OS on the JP1/AO server is Windows, the DNS Client service must be running before starting JP1/AO operations.

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

  In Windows, the default is *system-drive*`\Program Files\Hitachi\JP1AO`. You can change the installation folder.

  In Linux, the installation folder is `/opt/jp1ao` or `/var/opt/jp1ao`. You cannot change the installation folder.

- Database folder

  In Windows, the default is *system-drive*`\Program Files\Hitachi\HiCommand\database\Automation`. You can change the database folder.

  In Linux, the database folder is `/opt/HiCommand/database/Automation`. You cannot change the database folder.

- 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 22015. The protocol used for communication with Web browsers is HTTP.

Related topics

- New Installation in the JP1/Automatic Operation Configuration Guide

Appendix

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 (in Windows, Linux 6, Linux 7, SUSE Linux 12)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartweb	22/tcp[#1]	JP1/AO ➡ Operation target	Y	Used for SSH communications by the following functions: • Content plug-in (SSH connection) • General command plug-in (SSH connection) • File-transfer 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[#1]	JP1/AO ➡ Operation target	Y	Used for Telnet communications by the following functions: • 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 communication with Windows by the following functions: • Content plug-in (when the operation target is Windows)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartweb	445/tcp or 445/udp	JP1/AO ➡ Operation target	Y	• General command plug-in (when the operation target is Windows) • File-transfer plug-in (when the operation target is Windows)
cjstartweb	135/tcp	JP1/AO ➡ Operation target[#2]	Y	Used for communication with Windows by the following functions: • Content plug-in (when the operation target is Windows) • General command plug-in (when the operation target is Windows) • File-transfer plug-in (when the operation target is Windows)
cjstartweb	137/udp	JP1/AO ➡ Operation target[#3]	Y	Used for communication with Windows by the following functions: • Content plug-in (when the operation target is Windows) • General command plug-in (when the operation target is Windows) • File-transfer plug-in (when the operation target is Windows)
cjstartweb	25/tcp[#1]	JP1/AO ➡ SMTP server	Y	Used for sending emails by the following functions: • 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	22015/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	22016/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.
-	389/tcp[#1]	JP1/AO ➡ LDAP directory server	N	Used to connect to an LDAP directory server for Active Directory linkage.

Legend:

➡ : Unidirectional from left to right

Y: Registered as an exception during installation (in Windows).

N: Not registered as an exception during installation (in Windows and Linux).

#1

You can change this port number, if necessary. For details about the procedure, see Procedure to change the port number in the *JP1/AO Configuration Guide*.

#2

Only used with JP1/AO for Windows. Not used in JP1/AO for Linux.

#3

Only used with JP1/AO for Linux. Not used in JP1/AO for Windows.

Table A-2: List of port numbers for external connections (in Linux 8)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartsv	22/tcp[#1]	JP1/AO ➡ Operation target	Y	Used for SSH communications by the following functions: • Content plug-in (SSH connection) • General command plug-in (SSH connection) • File-transfer plug-in (SSH connection) • Terminal connect plug-in (SSH connection) • Terminal command plug-in (SSH connection) • Terminal disconnect plug-in (SSH connection)
cjstartsv	23/tcp[#1]	JP1/AO ➡ Operation target	Y	Used for Telnet communications by the following functions: • Terminal connect plug-in (Telnet connection) • Terminal command plug-in (Telnet connection) • Terminal disconnect plug-in (Telnet connection)
cjstartsv	445/tcp or 445/udp	JP1/AO ➡ Operation target	Y	Used for communication with Windows by the following functions: • Content plug-in (when the operation target is Windows) • General command plug-in (when the operation target is Windows) • File-transfer plug-in (when the operation target is Windows)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartsv	137/udp	JP1/AO ➡ Operation target[#2]	Y	Used for communication with Windows by the following functions: • Content plug-in (when the operation target is Windows) • General command plug-in (when the operation target is Windows) • File-transfer plug-in (when the operation target is Windows)
cjstartsv	25/tcp[#1]	JP1/AO ➡ SMTP server	Y	Used for sending emails by the following functions: • 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	22015/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	22016/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.
-	389/tcp[#1]	JP1/AO ➡ LDAP directory server	N	Used to connect to an LDAP directory server for Active Directory linkage.

Legend:

➡ : Unidirectional from left to right

Y: Registered as an exception during installation (in Windows).

N: Not registered as an exception during installation (in Windows and Linux).

#1

You can change this port number, if necessary. For details about the procedure, see Procedure to change the port number in the *JP1/AO Configuration Guide*.

#2

Only used with JP1/AO for Linux. Not used in JP1/AO for Windows.

(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-3: List of port numbers for internal connections (in Windows, Linux 6, Linux 7, SUSE Linux 12)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
cjstartweb	22029/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartweb	22030/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
httpsd	22031/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
pdrdmd	22032/tcp	JP1/AO ➡ JP1/AO	N	Used in a database of Common Component.
cjstartsv	22035/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22036/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22037/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22038/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.

Legend:

➡ : Unidirectional from left to right

N: Not registered as an exception during installation.

Table A-4: List of port numbers for internal connections (in Linux 8)

Service name	JP1/AO's port number	Firewall passage direction	Registered as an exception during installation?	Description
httpsd	22031/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
pdrdmd	22032/tcp	JP1/AO ➡ JP1/AO	N	Used in a database of Common Component.
cjstartsv	22035/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22036/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22037/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22038/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22170/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22171/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22172/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.
cjstartsv	22173/tcp	JP1/AO ➡ JP1/AO	N	Used in Common Component.

Legend:

➡ : Unidirectional from left to right

N: Not registered as an exception during installation.

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 *JP1/AO 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 *JP1/AO 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 *JP1/AO Service Template Reference*.

#

If the local execution function is enabled, the prerequisites do not have to be satisfied for the local host.

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
- Users who belong to the Administrator group[#1#2]
- Built-in Administrator of Active Directory
- Users who belong to the Domain Admin group of Active Directory[#1#2]

#1

Commands are executed using the permissions of the System account when a content plug-in is configured to be executed using System account permissions, and when true is specified for the runAsSystem property of a general command plug-in.

#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 R2.
- The OS is Windows Server 2012 or later.

Table A-5: 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-transfer plug-in
- Content plug-in

If administrative shares are disabled, specify the registry settings shown in the following table, and then restart the OS at the connection destination.

Table A-6: 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

To connect to a Windows connection destination from multiple JP1/AO servers, you must configure the property files of the connection destination. For details, see the "Connection-destination property file (connection-destination-name.properties)" in the document JP1/Automatic Operation Configuration Guide.

A.3 Version changes

(1) Changes in version 12-60

- Descriptions of the JP1/Base versions used for linking with other products were deleted.
- Descriptions of the local execution function were changed.
- The following operating systems are now supported:
  - Windows Server 2022
  - Red Hat Enterprise Linux 8
  - Oracle Linux 8
  - CentOS 8

- Port numbers were added to or deleted from the description of the ports used for JP1/AO external connections. Also, comments were added.
- Descriptions related to Linux were deleted from the descriptions of port numbers and the direction of the firewalls used for JP1/AO internal connections.
- The conditions for which registry settings are required for administrative shares were changed.
- The description of the important item when connecting to one Windows agentless connection destination from multiple JP1/AO servers was changed.

(2) Changes in version 12-01

- None

(3) Changes in version 12-00

- None

(4) Changes in version 11-10

- JP1/AO no longer requires JP1/Base as a prerequisite product, and descriptions of this requirement were deleted.
- JP1/AO no longer uses JP1/AJS3 as a task processing engine, and content indicating otherwise was deleted.
- Port numbers 22033/tcp and 22034/tcp were deleted from the list of ports used for JP1/AO internal connections, and port numbers 22035/tcp, 22036/tcp, 22037/tcp, and 22038/tcp were added.

(5) Changes in version 11-01

- jp1ajs2aoroot and HiRDBEmbeddedEdition_JF*n* were added to the list of port numbers (for internal connections).
- A note that commands will be executed using the permissions of the System account in certain circumstances was added. These circumstances are when a content plug-in is configured to be executed using the permissions of the System account, and when true is specified for the runAsSystem property of a general command plug-in.

(6) Changes in version 11-00

(a) Changes from the manual (3021-3-081-70)

- The following operating systems are now supported:
  - Linux 7
  - Oracle Linux 6 (x64)
  - Oracle Linux 7
  - CentOS 6 (x64)
  - CentOS 7
  - SUSE Linux 12
- The following operating systems are no longer supported:
  - Linux 5 (AMD/Intel 64)
  - Linux 5 Advanced Platform (AMD/Intel 64)
- The installation folder was changed for the Windows version of JP1/AO and the Common Component.

- A description of using JP1/AO in English and Chinese-language environments was added.
- The port numbers used for communication between JP1/AO and Web browsers were changed.
- *Tag management* was added as a way to classify service templates and services. Accordingly, category management was removed as a classification method.
- A Dashboard window was added in which users can view statistical information about services and tasks.
- Service groups were added as a way to manage resources. Accordingly, resource groups were removed.
- *Evaluating the working folders and execution directories for the operation-target devices* and *evaluating port numbers used for target devices* were added as tasks required for operation design.
- The name of a basic plug-in was changed from File-Forwarding Plug-in to File-Transfer Plug-in.
- The name of a basic plug-in was changed from Judge ReturnCode Plug-in to Branch by ReturnCode Plug-in.
- The name of a basic plug-in was changed from Judge Value Plug-in to Branch by Property Value Plug-in.

(b) Changes from the manual (3021-3-312-20(E))

- Linux was added as a supported operating system.
- The installation folder was changed for the Windows version of JP1/AO and the Common Component.
- The port numbers used for communication between JP1/AO and Web browsers were changed.
- A description of the local execution function was added. This function allows users to start processes directly on local hosts and perform tasks such as executing commands and copying files.
- Keyboard interactive authentication was added as an authentication method used for SSH connections with connection-target hosts.
- Information about the port number (22220/tcp) used for internal connections in an embedded database was added.
- The number of plug-ins that can be executed concurrently was changed to 110.
- *Tag management* was added as a way to classify service templates and services. Accordingly, category management was removed as a classification method.
- A Dashboard window was added in which users can view statistical information about services and tasks.
- Service groups were added as a way to manage resources. Accordingly, resource groups were removed.
- *Evaluating the working folders and execution directories for the operation-target devices* and *evaluating port numbers used for target devices* were added as tasks required for operation design.
- The name of a basic plug-in was changed from File-Forwarding Plug-in to File-Transfer Plug-in.
- The name of a basic plug-in was changed from Judge ReturnCode Plug-in to Branch by ReturnCode Plug-in.
- The name of a basic plug-in was changed from Judge Value Plug-in to Branch by Property Value Plug-in.

(7) Changes in version 10-52

(a) Changes in the manual (3021-3-081-70)

- Linux was added as a supported operating system.
- A description of the local execution function was added. This function allows users to start processes directly on local hosts and perform tasks such as executing commands and copying files.
- Keyboard interactive authentication was added as an authentication method used for SSH connections with connection-target hosts.
- Information about the port number (22220/tcp) used for internal connections in an embedded database was added.

- Information about the following port numbers used for internal connections in Common Component was added:
  - 23017/tcp
  - 23018/tcp
  - 23025/tcp
  - 23026/tcp
  - 23029/tcp
  - 23030/tcp
  - 23033/tcp
  - 23034/tcp
- Information about the port number (23032/tcp) used for internal connections in a Common Component database was added.
- The number of plug-ins that can be executed concurrently was changed to 110.

(8) Changes in version 10-50

(a) Changes in the manual (3021-3-081-60)

- Public key authentication was added as an authentication method used with operation target devices.
- It is now possible to use an API that calls JP1/AO functions from external programs.
- Linkage with Active Directory is now possible as external authentication linkage.
- The HTTPS protocol can now be used to establish a connection between a JP1/AO server and a Web browser.
- Information about the port number (139/tcp) used to establish a connection between a JP1/AO server and target devices was added.
- 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.

(b) Changes in the manual (3021-3-312-20(E))

- For the manual issued in December 2014 or later, the title and reference number were changed as shown below.

  Before the change:

  Job Management Partner 1/Automatic Operation GUI and Command Reference (3021-3-315(E))

  After the change:

  Job Management Partner 1/Automatic Operation GUI, Command, and API Reference (3021-3-366(E))
- It is now possible to use an API that calls JP1/AO functions from external programs.
- Windows Server 2012 R2 was added as an applicable operating system.
- Linkage with Active Directory is now possible as external authentication linkage.
- Public key authentication was added as an authentication method used with operation target devices.
- A method to specify whether a user who has logged in is elevated to a superuser was added to the following plug-ins:
  - General command plug-in
  - File-forwarding plug-in
  - Content plug-in

    - Terminal command plug-in
- Evaluations of work folders for operation target devices, and port numbers used by operation target devices, were added.
- Descriptions of debug services and debug tasks were added.
- The HTTPS protocol can now be used to establish a connection between a JP1/AO server and a Web browser.
- Information about the port number (139/tcp) used to establish a connection between a JP1/AO server and target devices was added.
- 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.

(9) Changes in version 10-12

(a) Changes in the manual (3021-3-081-50)

- Windows Server 2012 R2 was added as an applicable operating system.
- A method to specify whether a user who has logged in is elevated to a superuser was added to the following plug-ins:
    - General command plug-in
    - File-forwarding plug-in
    - Content plug-in
    - Terminal command plug-in
- Evaluations of work folders for operation target devices, and port numbers used by operation target devices, were added.
- Descriptions of debug services and debug tasks were added.

(10) Changes in version 10-11

(a) Changes in the manual (3021-3-081-40)

- It was stipulated that the description when SSH is selected as the protocol should apply to general command plug-ins, file-forwarding plug-ins, and content plug-ins.

(11) Changes in version 10-10

(a) Changes in the manual (3021-3-081-30)

- 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.

(b) Changes in the manual (3021-3-312-10(E))

- 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.

(12) Changes in version 10-02

(a) Changes in the manual (3021-3-081-20)

- A function for linking with JP1/AJS3 was added.
- Telnet was added as a protocol that can be used.
- The prerequisite OSs and software were added.

(13) Changes in version 10-01

(a) Changes in the manual (3021-3-081-10)

- The list of limit values of functions was added.

A.4 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):

- *JP1 Version 12 IT Operations Automation: Getting Started (3021-3-D01(E))*
- *JP1 Version 12 JP1/Automatic Operation Configuration Guide (3021-3-D03(E))*
- *JP1 Version 12 JP1/Automatic Operation Administration Guide(3021-3-D04(E))*
- *JP1 Version 12 JP1/Automatic Operation Service Template Developer's Guide (3021-3-D05(E))*
- *JP1 Version 12 JP1/Automatic Operation Command and API Reference(3021-3-D06(E))*
- *JP1 Version 12 JP1/Automatic Operation Service Template Reference (3021-3-D07(E))*
- *JP1 Version 12 JP1/Automatic Operation Messages (3021-3-D08(E))*

Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation	Full name or meaning
HCS	Hitachi Command Suite
HDvM or Device Manager	Hitachi Device Manager

Abbreviation		Full name or meaning
JP1/Cm2/NNM or JP1/Cm2/NNM-SE		JP1/Cm2/Network Node Manager Version 7 or earlier
		JP1/Cm2/Network Node Manager Starter Edition 250 Version 8 or earlier
		JP1/Cm2/Network Node Manager Starter Edition Enterprise Version 8 or earlier
JP1/Cm2/NNMi		JP1/Cm2/Network Node Manager i Version 9 or later
		JP1/Network Node Manager i version 11 or later
JP1/IM	JP1/IM - Manager	JP1/Integrated Management - Manager
		JP1/Integrated Management 2 - Manager
	JP1/IM - View[#1]	JP1/Integrated Management - View
		JP1/Integrated Management 2 - View
JP1/IM - NP		JP1/Integrated Management - Navigation Platform
		JP1/Navigation Platform
JP1/IM - SS		JP1/Integrated Management - Service Support
		JP1/Service Support
JP1/OA		JP1/Operations Analytics
JP1/PFM		JP1/Performance Management
JP1/PFM - Base		JP1/Performance Management - Base
JP1/PFM - Manager		JP1/Performance Management - Manager
JP1/PFM - RM		JP1/Performance Management - Remote Monitor for Microsoft(R) SQL Server
		JP1/Performance Management - Remote Monitor for Oracle
		JP1/Performance Management - Remote Monitor for Platform
JP1/PFM - WebConsole		JP1/Performance Management - Web Console
Tuning Manager		Hitachi Tuning Manager
UNIX	HP-UX	HP-UX 11i V3 (IPF)
	Linux[#2]	Linux (R)
	Solaris	Solaris 10 (SPARC)
		Solaris 11 (SPARC)
vCenter		VMware vCenter(TM) Server
VMware		VMware(R)

#1

JP1/IM - View version 11 or later is the name of a breakdown model of JP1/IM - Manager.

#2

This is the notation for pertaining to the OS of an operation-target device. The notation for pertaining to the OS of a JP1/AO server is as follows:

Abbreviation			Full name or meaning
Linux	Linux 6	CentOS 6 (x64)	Community ENTerprise Operating System 6 (x64)
		Oracle Linux 6 (x64)	Oracle Linux(R) Operating System 6 (x64)
		Red Hat Enterprise Linux 6 (x64)	Red Hat Enterprise Linux(R) Server 6 (64-bit x86_64)
	Linux 7	CentOS 7	Community ENTerprise Operating System 7
		Oracle Linux 7	Oracle Linux(R) Operating System 7
		Red Hat Enterprise Linux 7	Red Hat Enterprise Linux(R) Server 7
	Linux 8	CentOS 8	Community ENTerprise Operating System 8
		Oracle Linux 8	Oracle Linux(R) Operating System 8
		Red Hat Enterprise Linux 8	Red Hat Enterprise Linux(R) Server 8
	SUSE Linux 12		SUSE Linux(R) Enterprise Server 12

Conventions: Acronyms

This manual uses the following acronyms:

Acronym	Full name or meaning
AIX	Advanced Interactive Executive
API	Application Programming Interface
ASCII	American standard code for information interchange
AWS	Amazon Web Services
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

Acronym	Full name or meaning
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
IP	Internet Protocol
IPF	Itanium(R) Processor Family
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
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

Acronym	Full name or meaning
RFC	Request For Comment
RPC	Remote Procedure Call
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
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
VM	Virtual Machine
VMFS	Virtual Machine File System
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 $1{,}024^2$ bytes. 1 GB (gigabyte) is $1{,}024^3$ bytes. 1 TB (terabyte) is $1{,}024^4$ bytes.

Glossary

A

Admin role

A type of role. The user group for which this role is set can manage service groups, and manage and develop service templates. It can also manage 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

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 also 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.

Component

Plug-ins and release service templates that can be placed as steps in the flow of a service template.

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 service groups.

D

debug service
: A service that is generated and run when a Development service template is debugged. Unlike ordinary services, debug services need not be created in the **Service Definition** (Create) window or run in the **Submit Service** window.

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.

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

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.

Develop role
: A type of role. The user group for which this role is set can manage and develop service templates, and manage and 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 window immediately after login. The following three windows can be displayed: **Service Definition** (Edit) window, **Submit Service** window, and **Task Details** window.

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.

J

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

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 resource group
: In JP1/Base, the management targets (resources), such as jobs 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.

JP1/AO Content Pack
: 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/Cm2/NNMi
: Product for achieving integrated network management, such as network configuration management, performance management, and failure management.

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.

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

A type of role. The user group for which this role is set can manage 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 Pack 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** area.

profile

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

Property mapping

Settings for inheriting property values between step properties or between a step property and a service property. For example, you can specify the settings so that the value of an output property of the previous step is inherited to the value for an input property of the next step.

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.

Related step

When a step property is elevated to a service property, the original step is called the *related step* for the service property. Also, when a property group in a service component is based on another service component, a step that uses the other service component is called the *related step* for the property group.

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. A release service template can also be placed as a service component in the flow when a service template is developed.

repeated step

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

role

Attribute used to restrict operations (such as managing and running services) for a given service group from a user group. There are four roles: 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 component

Release service templates that can be placed as steps in the flow of a service template. The release service templates imported to JP1/AO can be placed as service components in the flow.

Service group

A group of services and connection destinations.

Service property

Properties used by users who submit services to specify the values necessary for submitting the services, or to acquire the submission results of the services. Service properties include input properties, output properties, and variables.

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.

Step property

Internal properties used to specify values necessary for executing steps, or to acquire the execution results of the steps.

Submit role

A type of role. The user group for which this role is set can run services.

T

Tag

Category information (such as the purpose of use and the type) of services. Service templates, services, and tasks are classified based on this information. The classification includes the large classification (by tag group) and the small classification (by tag).

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-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 service group and have the same permissions for that service 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

Admin role (glossary) 74
administrative share setting 64
archive (glossary) 74

B

build (glossary) 74
built-in user group (glossary) 74

C

cluster system (glossary) 74
Common Component (glossary) 74
component (glossary) 74
connection destination
  prerequisites 62
  users who can connect to 63
connection destination (glossary) 74

D

debug service (glossary) 75
debug task (glossary) 75
debugger (glossary) 75
debugging (glossary) 75
design procedure 35
Develop role (glossary) 75
development plug-in (glossary) 75
development service template (glossary) 75
direct-access URL (glossary) 75

E

external authentication linkage (glossary) 75

F

flow (glossary) 75
function
  for automating operation procedures 22
  for linking with other products 27
  for managing operation targets 25
  for monitoring automated operation procedures 24
  introduction to 21

H

history (glossary) 76
Hitachi Command Suite (glossary) 76

J

job (glossary) 76
JP1 event (glossary) 76
JP1 resource group (glossary) 76
JP1 user (glossary) 76
JP1/AO
  benefit of deployment 15
  example application 17
  overview 13
JP1/AO Content Pack (glossary) 76
JP1/AO system
  designing 32
  lifecycle 33
JP1/Automatic Operation (glossary) 76
JP1/Cm2/NNMi (glossary) 76
JP1/Integrated Management (glossary) 76
JP1/Performance Management (glossary) 76

L

layering step (glossary) 77
LDAP search user (glossary) 77

M

Modify role (glossary) 77

N

normal step (glossary) 77

O

operation design 42
  evaluating audit logs 50
  evaluating error handling 50
  evaluating maintenance 50
  evaluating method of executing plug-ins 45
  evaluating operations for access control by device 44
  evaluating operations using external authentication linkage 43
  evaluating operations using groups 43
  evaluating port numbers used for target devices 47

evaluating status notification method 49
evaluating task retention period 48
evaluating users and access permissions 42
evaluating working folders and execution directories for operation-target devices 46
operation design procedure 36
operation procedure to be automated
evaluating 38
operation procedure using JP1/AO 18

P

plug-in (glossary) 77
plug-in icon file (glossary) 77
port
used for JP1/AO external connections 58
used for JP1/AO internal connections 61
port numbers, list of 58
profile (glossary) 77
property mapping (glossary) 77

R

reference information 58
related line (glossary) 77
related step (glossary) 78
release (glossary) 78
Release plug-in (glossary) 78
release service template (glossary) 78
repeated step (glossary) 78
role (glossary) 78

S

service (glossary) 78
service component (glossary) 78
service design 38
evaluating items to be considered when services are added 39
evaluating items to be specified when services are run 40
evaluating shared service properties 40
service design procedure 36
service group (glossary) 78
service property (glossary) 78
service template (glossary) 79
service template to be used
evaluating 38
shared service property (glossary) 79
step (glossary) 79
step property (glossary) 79
Submit role (glossary) 79
system design 52
checking operating environment 55
evaluating details of installation 56
evaluating network settings 54
evaluating system configuration 52
system design procedure 37
system operation, challenge faced by 14

T

tag (glossary) 79
task (glossary) 79
task-processing engine (glossary) 79

U

user group (glossary) 79
User Management permission (glossary) 79

Hitachi, Ltd.
6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan