HITACHI
Inspire the Next

JP1 Version 11

JP1/Operations Analytics Configuration and Administration Guide

3021-3-B92-20(E)

Notices

■ Relevant program products

P-2A2C-DCBL JP1/Operations Analytics 11-50 (for Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016)

■ Trademarks

HITACHI, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.
Brocade is a trademark or a registered trademark of Brocade Communications Systems, Inc. in the United States and/or in other countries.
Cisco is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.
IBM, AIX are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.
Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries.
Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.
Microsoft and Hyper-V are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
Oracle and Java are registered trademarks of Oracle and/or its affiliates in the United States and/or other countries.
Red Hat is a trademark or a registered trademark of Red Hat Inc. in the United States and other countries.
RSA and BSAFE are either trademarks or registered trademarks of EMC Corporation in the United States and/or other countries.
SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.
Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.
Other company and product names mentioned in this document may be the trademarks of their respective owners.
JP1/Operations Analytics includes RSA BSAFE(R) Cryptographic software of EMC Corporation.
This product includes software developed by the Apache Software Foundation (http://www.apache.org/).
This product includes software developed by Ben Laurie for use in the Apache-SSL HTTP server project.
This product includes software developed by IAIK of Graz University of Technology.
Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.
This product includes software developed by the University of California, Berkeley and its contributors.
This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm, including

various modifications by Spyglass Inc., Carnegie Mellon University, and Bell Communications Research, Inc (Bellcore).

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

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

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 Daisuke Okajima and Kohsuke Kawaguchi (http://relaxngcc.sf.net/).

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

■Microsoft product name abbreviations

This manual uses the following abbreviations for Microsoft product names.

Abbreviation		Full name or meaning
Hyper-V		Microsoft(R) Windows Server(R) 2008 R2 Hyper-V(R) Microsoft(R) Windows Server(R) 2012 Hyper-V(R) Microsoft(R) Windows Server(R) 2012 R2 Hyper-V(R) Microsoft(R) Windows Server(R) 2016 Hyper-V(R)
Internet Explorer		Windows(R) Internet Explorer(R)
PowerShell		Windows PowerShell
Visual C++		Microsoft(R) Visual C++(R)
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	Microsoft(R) Windows Server(R) 2012 Datacenter
		Microsoft(R) Windows Server(R) 2012 Standard
	Windows Server 2012 R2	Microsoft(R) Windows Server(R) 2012 R2 Datacenter
		Microsoft(R) Windows Server(R) 2012 R2 Standard
Windows Server 2016		Microsoft(R) Windows Server(R) 2016 Datacenter
		Microsoft(R) Windows Server(R) 2016 Standard

Windows is sometimes used generically, referring to Windows Server 2008 R2, Windows Server 2012, and Windows Server 2016.

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

■ Edition history

Nov. 2017: 3021-3-B92-20(E)

■ Copy right

Summary of amendments

The following table lists changes in this manual (3021-3-B92-20(E)) and product changes related to this manual.

Changes	Location
The HAnalytics Engine Database _OA0 service was added to each procedure for setting up the JP1/OA services in cluster software.	1.1.2(1), 1.2.3, 2.3.2, 2.3.4, 2.3.8, 3.2.3(4), 3.2.4(2), 3.2.4(4), 3.2.5(3)
In the `user_httpsd.conf` file example, the content of the SSLRequiredCiphers directive was changed.	1.3.3
The `AD.inventory.ipSwitch.portsToRemove` key was added to the system property file (Argus.properties).	1.4.2
Conditions for writing a definition file to display % were deleted or changed.	1.5.3(3), 4.5.3, 4.7.3
Descriptions of the **Event Analysis View** window and the **Performance Analysis View** window were added for the function for outputting resource information.	2.1.2, 2.1.3
Descriptions of how to import JP1/PFM reports and performance information from other software and to then display the imported performance information in performance graphs were added.	2.2
A description for collecting JP1 events from JP1/IM was added to the procedure for linking with a Windows edition of a JP1 product.	4.2
A procedure for linking with a UNIX edition of a JP1 product was added.	4.3
The following descriptions were added to the descriptions for the email template definition files and the command template definition files: - The `SE.template.filter.groups.string` key was added to the settings. - `%ANALYTICS_GROUPS%` was added to the list of usable fill character variables.	4.5.3, 4.7.3
Settings for which fill character variables can be used were specified in the explanation of the formats of email template definition files and command definition files.	4.5.3, 4.7.3
Descriptions related to application monitoring were added. In accordance with this, the following additions or changes were made: - The descriptions of the arguments and return values for the `addsetting` command, `deletesetting` command, and `updatesetting` command were changed. - The items output to CSV files as basic information and event information were added.	6, 7.7.2, 7.7.3, 7.7.18, Appendix F. (2), Appendix F. (5), Appendix I.
The following changes or additions were made regarding the `reloadproperty` command: - The description of the command was changed. - Definition files referenced by the command were added. - The location of the command was modified.	7.1, 7.7.16
SHA512withRSA was added as a specifiable value for the `sigalg` option of the `hcmds64ssltool` command.	7.6.5

Changes	Location
The items and item names in the file output by the `listconsumers` command were changed.	7.7.10
Notes on the `outputevent` command now specify how to deal with the situation in which a large number of events are output.	7.7.12
The free capacity required for the temporary directory when the `expandretention` command is executed was changed.	7.8.2
The names of the log files that can be acquired by the logtypes option of the `hcmds64getlogs` command were modified.	7.8.3
The following port numbers used for external connections in JP1/OA were changed: - Port number 445/tcp, which was used when registering the monitoring target that uses WMI for monitoring, was deleted. - Port number 3389/tcp, which was used when the following software was registered as management software, was deleted: - JP1/AJS3 - JP1/IM - JP1/PFM - Port number 20700/tcp, which was used when registering JP1/IM, was added.	Appendix B. (1)
The following information was added to Performance Information Collected by JP1/OA. - Amount of compressed memory - Speed at which memory is swapped in - Speed at which memory is swapped out - Wait time for kernel commands - Speed at which memory for virtual machines is swapped in - Speed at which memory for virtual machines is swapped out - Disk usage for virtual machines - Disk usage for virtual machines (reserved)	Appendix C.
A note on setting Windows Server 2016 as a management target was added.	Appendix D. (3)
The format of the URL of an SMI-S provider, specified when using the SMI-S provider connection check tool, was changed.	Appendix H. (3)
The following output items (in CSV files to which resource information is output) were added to the structure of the body section that indicates basic information: - Execution Agent Name - Maximum Number of Concurrently Executable Jobs - Execution Agent Group Name Execution Agent List was added to the information output in Resource Information Type.	Appendix F. (2)
A description of the format of CSV files used by commands that perform setting operations was added.	Appendix G.

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

Preface

This manual describes the functionality and operation of JP1/Operations Analytics.

■Intended readers

This manual is intended for:

- System administrators who are responsible for introducing and operating JP1/Operations Analytics.

■Organization of this manual

PART 1: Configuration

This part describes the procedures for overwrite installation, upgrade installation, and uninstallation.

PART 2: Administration

This part describes the procedures required in operation.

PART 3: System design

This part describes the procedures for creating cluster systems.

PART 4: Linking to other products

This part describes the procedure for linking with other products.

PART 5: Direct Access URL

This part describes the function used to directly display a specific operation window immediately after login by specifying the URL of the operation window.

PART 6: Application monitoring

This part describes how to register applications to be monitored by JP1/OA, and how to customize what is to be monitored.

PART 7: Commands

This part describes the commands used in JP1/OA.

PART 8: Troubleshooting

This part describes the cause and what to do if a problem occurs while you are using JP1/OA.

APPENDIX A: JP1/OA Services

This part describes the JP1/OA services registered when JP1/OA is installed.

APPENDIX B: Port Numbers Used by JP1/OA

This part lists the port numbers to be set and the direction in which communication passes through the firewall over the ports.

APPENDIX C: Performance Information Collected by JP1/OA

This part describes the performance information that is collected by JP1/OA.

APPENDIX D: List of resources managed by JP1/OA

This part describes the resources managed by JP1/OA.

APPENDIX E: List of Limits

This part describes the various restrictions imposed by JP1/OA.

APPENDIX F: Format for the Output of Resource Information to CSV Files

This part describes the format used when resource information is output to a CSV file.

APPENDIX G: Format for the Output of Setting Information to CSV Files

This part describes the format of CSV files used by commands that perform setting operations.

APPENDIX H: How to Use the SMI-S Provider Connection Check Tool

This part describes the SMI-S provider connection tool.

APPENDIX I: How to Use sample collectors

This part describes the procedure for monitoring applications by using sample collectors.

APPENDIX J: Version Changes

This part describes the changes in each version.

■Reading procedure

Use the following table as a guide in selecting the sections that meet your purposes.

No.	Purpose	Relevant sections
1	Configuring JP1/OA	Part 1 Configuration
2	Using JP1/OA	Part 2 Administration
3	Creating cluster systems	Part 3 System design
4	Linking JP1/OA with other products	Part 4 Linking to other products
5	Directly displaying the desired window by specifying the URL of the operation window	Part 5 Direct Access URL
6	Customizing the settings for application monitoring, and what is to be monitored	Part 6 Application Monitoring
7	Finding out how to use commands	Part 7 Commands
8	Finding out what action to take if a problem occurs	Part 8 Troubleshooting

■Conventions: Directory names

HP-UX directory names are used in this manual as a general rule. The directory names have symbolic links, so that users of UNIX OSs other than HP-UX can use the same directory names.

When HP-UX uses a different directory name from another flavor of UNIX, both directory names are given.

■Conventions: Fonts and symbols

The following table explains the text formatting conventions used in this manual:

Text formatting	Convention
Bold	Bold characters indicate text in a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italic	Italic characters indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` Italic characters are also used for emphasis. For example: • Do *not* delete the configuration file.
`Monospace`	Monospace characters indicate text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed: `The password is incorrect.`

The following table lists the conventions used in syntax explanations:

Symbol	Convention
`|`	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means `A`, or `B`, or `C`.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of `A`, or `B`, or `C`.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (...) indicates that one or more lines of coding have been omitted. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify `B` as many times as necessary.

■Terms used in this manual

This manual uses the following terms:

Term	Description
Installation destination folder of JP1/OA	The folder into which JP1/OA is installed. The default installation destination is C:\Program Files\HITACHI\JP1OA.
Common component	The component shared by several products and used by JP1/OA. The common component is shared between JP1/OA and JP1/Automatic Operation, or between JP1/OA and Hitachi Command Suite products.
Common component of installation destination folder	The folder into which the common component is installed. When JP1/OA is installed, this folder is created automatically. The default installation destination is C:\Program Files\HITACHI\HiCommand\Base64. If one or more products that use the common component have already been installed, the folder in which those products are installed is used.

■Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names.

Abbreviation	Full name or meaning
Firefox	Firefox(R)
JP1/AJS3	JP1/Automatic Job Management System 3
JP1/AO	JP1/Automation Director
JP1/IM	JP1/Integrated Management
JP1/NP	JP1/Navigation Platform
JP1/OA	JP1/Operations Analytics
JP1/PFM	JP1/Performance Management
JP1/SS	JP1/Service Support
Linux	A generic term used to refer to the following OSs monitored by JP1/OA: CentOS, Oracle Linux(R), Red Hat Enterprise Linux(R), and SUSE Linux(R)
UNIX	UNIX(R)
vCenter Server or vCenter	VMware vCenter Server(R)
VMware	VMware(R)
VMware ESXi or ESX	VMware vSphere(R) ESXi(TM)

■Conventions: Acronyms

This manual uses the following acronyms.

Acronym	Full name or meaning
CA	Certification Authority
CPU	Central Processing Unit
CSR	Certificate Signing Request
CSV	Character Separated Values
DBMS	Database Management System
DN	Domain Name
DNS	Domain Name System
ECC	Elliptic Curve Cryptography
FC	Fibre Channel
GUI	Graphical User Interface
HBA	Host Bus Adapter
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LAN	Local Area Network
LUN	Logical Unit Number
MIB	Management Information Base
NIC	Network Interface Card
OS	Operating System
PEM	Privacy Enhanced Mail
SMI-S	Storage Management Initiative - Specification
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TSV	Tab Separated Values
UAC	User Account Control
UDP	User Datagram Protocol
UNC	Universal Naming Convention
UUID	Universally Unique Identifier
URL	Uniform Resource Locator
VM	Virtual Machine
WBEM	Web-Based Enterprise Management

Acronym	Full name or meaning
WMI	Windows Management Instrumentation
WWN	World Wide Name

■Conventions: "Administrator permissions" as used in this manual

In this manual, *Administrator permissions* refers to Administrator permissions for the local PC. The local user, domain user, or user of the Active Directory environment can perform tasks requiring Administrator permissions if granted Administrator permissions for the local PC.

■Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

Contents

1.Configuration

This chapter describes how to perform an overwrite installation or upgrade installation of JP1/Operations Analytics, and how to uninstall the product. These operations are also applicable to cluster configurations.

For details about how to install the product for the first time, see the *JP1 Version 11 Integrated Management Getting Started (IT Operations Analytics)*. For details about how to install the product for the first time in the case of a cluster system, see *3.2 Establishing JP1/OA in a cluster system*.

1.1 Overwrite or upgrade installation

Overwrite installation refers to an installation of the same version of the product on the computer on which the product has already been installed.

Upgrade installation refers to installation of a later version of the product on a computer where the product has already been installed.

The same procedure can be used for both an overwrite installation and upgrade installation.

1.1.1 Performing an overwrite installation or an upgrade installation of JP1/OA (in the case of a non-cluster system)

Log in to the system as a user that has the Administrator permission and perform the following operation:

1. Backup the JP1/OA system.
   For details on how to back up the JP1/OA system, see *2.3.1 Backing up data in a JP1/OA system (non-cluster configuration)*.
2. Start the installation program from the provided medium.
3. Specify settings according to the installation wizard.
4. Install JP1/OA.

The installation is completed when the JP1/OA service starts.

1.1.2 Performing an overwrite installation or an upgrade installation of JP1/OA (in the case of a cluster system)

In the case of a cluster system, an overwrite installation or an upgrade installation must be performed on both the active server and the standby server.

(1) Installation preparations:

1. Use the cluster software to move the resource group where the JP1/OA services are registered to the active server.
2. Backup the JP1/OA system on the active server.
   For details on how to back up the JP1/OA system, see *2.3.2 Backing up data in a JP1/OA system (cluster configuration)*.
   If you backed up the JP1/OA system by using the above procedure, failover for the services registered in the cluster software will be suppressed.

3. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
4. Use the cluster software to move the resource group where the JP1/OA service is registered to the standby server.
5. Use the cluster software to bring the above resource group online.
6. Use the cluster software to bring the services offline.

   If the JP1/AO or the Hitachi Command Suite products are installed, bring all services offline except for the following services:

   - HiRDB/ClusterService _HD1

   If the JP1/AO or the Hitachi Command Suite products are not installed, bring the following services offline:

   - HAnalytics Engine Database _OA0
   - HAnalytics Engine Cluster Database _OA0
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
7. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
8. Use the cluster software to bring the following services offline:
   - HiRDB/ClusterService _HD1

(2) Installing JP1/OA on the active server and the standby server

1. Use the cluster software to move the resource group where the JP1/OA services are registered to the active server.
2. Install JP1/OA on the active server.
3. Use the cluster software to move the resource group where the JP1/OA services are registered to the standby server.
4. Install JP1/OA on the standby server.

(3) Enabling failover (in Windows):

1. Use the cluster software to move the resource group where the JP1/OA services are registered to the active server.
2. In the cluster software, enable failover for the resource group where the JP1/OA services are registered.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the following settings:

   - The setting for attempting a restart on the current node if the resources fails
   - The setting for failing over all resources in the target service or application if a restart fails

   Perform this action for all services registered in the resource group in order to enable failover.
3. Bring the resource group where the JP1/OA services are registered online by using the cluster software.

1.2 Uninstallation

1.2.1 Preparation for uninstallation

Before uninstalling JP1/OA, you must release or change the settings.

To uninstall the product:

Log in to the system as a user that has the Administrator permission and perform the following operation:

1. Stop the security monitoring software, antivirus software, and process monitoring software.
   If these software programs are running, the uninstallation might fail because a process in progress might be blocked from access by the uninstallation program.
2. If the services of products that use Common Component are running, stop them.
   If you start the uninstallation while the services of products that use common components are running, a dialog box prompting you to stop those services appears.
3. Set **Startup type** for the JP1/OA service to **Automatic** or **Manual**.
   If **Startup type** for related services is set to **Disabled** when you perform the uninstallation in Windows, the uninstallation fails because those services cannot be started. Therefore, you must set **Startup type** to **Automatic** or **Manual**.

For details about the JP1/OA service, see *Appendix A. JP1/OA Services*.

1.2.2 Uninstalling JP1/OA (in the case of a non-cluster system)

Uninstall JP1/OA from **Programs and Features** in Control Panel.

1. Click **Programs** and then **Programs and Features** in Control Panel, select JP1/Operations Analytics, and then click **Uninstall**.
2. JP1/OA will be uninstalled.

When you uninstall JP1/OA, the settings files in the installation folder are not deleted because those files store the settings that might be needed for future installations. You must back up or delete these settings files as necessary.

1.2.3 Procedure to uninstall JP1/OA (in the case of a cluster system)

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

To configure services before uninstallation:

Configure services on the active server before uninstallation.

1. Use the cluster software to move the resource group where the JP1/OA service is registered to the active server.
2. Use the cluster software to bring the above resource group online.

3. Use the cluster software to bring the services offline.
   If the JP1/AO or the Hitachi Command Suite products are installed, bring all services offline except for the following services:
   - HiRDB/ClusterService _HD1

   If the JP1/AO and the Hitachi Command Suite products are not installed, bring the following services offline:
   - HAnalytics Engine Database _OA0
   - HAnalytics Engine Cluster Database _OA0
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
4. On the active server, execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
5. If the following service is not offline, place it offline by using the cluster software:
   - HiRDB/ClusterService _HD1
6. In the cluster software, suppress failover for the resource group.
   Right-click a service or script in the cluster software, select Properties, and then Policies. Then, specify the settings so that a restart does not occur if the resource fails. Perform this action for all services and scripts registered in the resource group in order to suppress failover.

To uninstall JP1/OA:

Uninstall JP1/OA.

1. Use the cluster software to move the resource group where the JP1/OA service is registered to the active server.
2. Uninstall JP1/OA from the active server.
3. Uninstall JP1/OA from the standby server.
   The shared disk does not need to be available on the standby server.

When you uninstall JP1/OA, the settings files in the installation folder are not deleted because those files store the settings that might be needed for future installations. You must back up or delete these settings files as necessary.

To delete services from the cluster software:

Delete services from the cluster software.

1. Use the cluster software to delete from the resource group any of the following script and services that are not used by other applications:
   - HAnalytics Engine
   - HAnalytics Engine Web Service

- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- HAnalytics Engine Database _OA0
- HAnalytics Engine Cluster Database _OA0
- HiRDB/ClusterService _HD1

2. If you want to continue to use the remaining services and scripts, use the cluster software to enable failover for the resource group.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if a resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.

1.3 Enabling HTTPS connections between the web browser and JP1/OA

1.3.1 Methods of communication with the web browser that are available in JP1/OA

You can choose HTTP or HTTPS connections for connections between the web browser and JP1/OA. To use an HTTPS connection, you need to obtain the SSL server certificate from a CA (certification authority) and specify the settings to enable HTTPS connections.

In JP1/OA, HTTP connections are set by default.

1.3.2 Obtaining the SSL server certificate required for HTTPS connections

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

Preparation:

Log in to the JP1/OA server as a user that has the Administrator permission.

To obtain the SSL server certificate:

1. Execute the `hcmds64ssltool` command, and save a private key file and a CSR file, which needs to be sent to a CA.
2. Send the saved CSR file to a CA and obtain the SSL server certificate file (PEM format).

Important note:

SSL server certificate issued by a CA have an expiration date. You need to have a certificate reissued before your certificate expires.

To check the expiration date, use the `hcmds64checkcerts` command.

1.3.3 Enabling HTTPS connections

Configure the user_httpsd.conf file, store the private key file and SSL server certificate file in the specified folder, and enable HTTPS connections on the web server.

Preparation:

- Log in to the JP1/OA server as a user that has the Administrator permission.
- Stop the JP1/OA service.

To enable HTTPS connections:

1. Change the settings in the user_httpsd.conf file so that HTTPS connections can be used.
   The user_httpsd.conf file is stored in the following folder:

   Common-Component-installation-folder`\uCPSB\httpsd\conf`

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

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

Note:

Note the following when editing the directives:

- The SSL server certificate file and private key file can be stored in folders in the *Common-Component-installation-folder* and also in any folder specified as a storage folder in the user_httpsd.conf file. Do not include junctions or symbolic links in the specified folder.
- Do not specify the same directive twice.
- Do not enter a line break in the middle of a directive.

The following shows the settings in the user_httpsd.conf file after JP1/OA is installed (HTTP connections are used), and the settings in the user_httpsd.conf file that are changed to use HTTPS connections.

<Before the change>

```
ServerName JP1/OA-server-name
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
SSLDisable
#Listen 22016
#Listen [::]:22016
#<VirtualHost *:22016>
#  ServerName JP1/OA-server-name
#  SSLEnable
#  SSLProtocol TLSv12
#  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:AES256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256
#  SSLRequireSSL
#  SSLCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem"
#  SSLCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/httpsd.pem"
#  SSLECCCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/ecc-httpsdkey.pem"
#  SSLECCCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.pem"
#  SSLCACertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#</VirtualHost>
#HWSLogSSLVerbose On
```

<After the change>

```
ServerName JP1/OA-server-name
#Listen 22015 #1
#Listen [::]:22015 #1
Listen 127.0.0.1:22015 #2
SSLDisable
Listen 22016 #2
Listen [::]:22016 #2
<VirtualHost *:22016> #2
  ServerName JP1/OA-server-name #2
  SSLEnable #2
  SSLProtocol TLSv12 #2
  SSLRequiredCiphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:
ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-GCM-SHA38
4:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:AE
S256-GCM-SHA384:AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256 #2
  SSLRequireSSL #2
  SSLCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/httpsdkey.pem
" #2
  SSLCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/httpsd.pem" #2
#  SSLECCCertificateKeyFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/ecc-http
sdkey.pem" #3
#  SSLECCCertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/server/ecc-httpsd.p
em" #3
#  SSLCACertificateFile "Common-Component-installation-folder/uCPSB/httpsd/conf/ssl/cacert/anycert.pem"
#4
</VirtualHost> #2
HWSLogSSLVerbose On #2
```

#1: This directive is unnecessary if HTTPS connections are used. Add a hash mark (#) at the beginning of the line to comment out the line.

#2: This directive is necessary for using HTTPS connections. Delete the hash mark (#) at the beginning of the line to enable the directive.

#3: This directive is necessary for using an SSL server certificate with elliptic curve ciphers (ECC) via an HTTPS connection. If necessary, delete the hash mark (#) at the beginning of the line to enable the directive.

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

2. For the SSLCertificateFile directive, specify the location of the SSL server certificate file for the RSA cipher by using an absolute path.

   Store the SSL server certificate file for the RSA cipher in the path specified by the SSLCertificateFile directive in the user_httpsd.conf file.

3. For the SSLCertificateKeyFile directive, specify the location of the private key file for the RSA cipher by using an absolute path.

   Store the private key file for the RSA cipher in the path specified by the SSLCertificateKeyFile directive in the user_httpsd.conf file.

4. To use an SSL server certificate with elliptic curve ciphers, perform steps 5 and 6.

Important note:
If you updated from version 11-00 of JP1/OA, you must apply the directive for the elliptic curve ciphers to the user_httpsd.conf file.
Apply the directive by copying the contents of the SSLRequiredCiphers directive, the SSLECCCertificateKeyFile directive, and the SSLECCCertificateFile directive from the sample file stored in the following location:

Common-Component-installation-folder`\sample\httpsd\conf\user_httpsd.conf`

5. For the SSLECCCertificateFile directive, specify the location of the SSL server certificate file for elliptic curve ciphers by using an absolute path.

   Store the SSL server certificate file for elliptic curve ciphers in the path specified by the SSLECCCertificateFile directive in the user_httpsd.conf file.
6. For the SSLECCCertificateKeyFile directive, specify the location of the private key file for elliptic curve ciphers by using an absolute path.

   Store the private key file for elliptic curve ciphers in the path specified by the SSLECCCertificateKeyFile directive in the user_httpsd.conf file.
7. To use the SSL server certificate file issued by the chained CA, use the SSLCACertificateFile directive to specify the location of the chained CA certificate file by using an absolute path.

   Multiple certificates can be contained in one file by chaining multiple certificates (in PEM format) by using a text editor. Note that you must not specify symbolic links or junctions for the path.
8. Execute the `hcmds64fwcancel` command to register firewall exceptions.
9. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

1.3.4 Configuring the HTTP port used by commands

If you change the port number used for communications between JP1/OA and the web browser, you also need to change the HTTP port to be used by commands to the same port number.

1. Edit the command properties file. The command properties file is as follows:

   Storage folder:

   For non-cluster systems:

   installation-destination-folder-of-JP1/OA`\conf`

   For cluster systems:

   shared-folder-name`\Analytics\conf`

   File name: command_user.properties

   Change the value of the command.ssl property from "false" to "true".

<Before the change>

```
command.ssl = false
command.http.port = 22015
command.https.port = 22016
```

<After the change>

```
command.ssl = true
command.http.port = 22015
command.https.port = 22016
```

1.4 Post-Installation Environment Settings

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

1.4.1 Procedure for setting the JP1/OA environment

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

To set the JP1/OA environment:

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

Table 1-1 Settings and their definition files

Settings	Definition file to use	Reference
Various settings such as port numbers	System property file (Argus.properties)	1.4.2 System property file (Argus.properties)
Settings for event action	Event action definition file (EventAction.properties)	1.4.3 Event action definition file (EventAction.properties)
Settings for other products linkage	Mail template definition file	1.4.4 Mail template definition file
	Command template definition file	1.4.5 Command template definition file

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

1.4.2 System property file (Argus.properties)

This is the definition file used for various settings such as port numbers.

Format

specification-key-name = setting

Installation folder

For non-cluster systems:

installation-destination-folder-of-JP1/OA \JP1OA\conf

For cluster systems:

shared-folder-name\Analytics\conf

Trigger for applying definitions

Restarting the JP1/OA service

Description

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

- Lines that begin with a hash mark (#) are treated as comments.
- Blank lines are ignored.
- The encoding is ISO 8859-1.
- The entries are case sensitive.

Settings

Table 1-2 Settings in the property file

Key name	Settings	Specifiable values	Default value
CO.DBPortNo	Specifies the port number used for the database of this product.	1 to 65535	27102
CO.rmi.registoryPort	Specifies the port number used among services of this product.	1 to 65535	27104
SE.event.maxCurrentEventResult	Specifies the maximum number of events that can be sent by the email notification function (Notification Settings] in the [Administration] tab).	1 to 65535	50
SE.event.maxEventLogRetentionDays	Specifies the number of days that an event is retained. If 0 is specified, the duration is not limited.	0 to 1000	126
SE.cluster.logicalHostName	Specifies the logical host name in a cluster system environment.	32 or fewer bytes: alphanumeric characters, hyphens (-)	Null string
AD.inventory.ipSwitch.portsToRemove	Specifies the character string included in the name of a port. You can specify several character strings by using a virtual bar (|) as a delimiter.	Character string of 1000 or fewer bytes. No restriction on the types of characters.	VLAN|vlan|Vlan

1.4.3 Event action definition file (EventAction.properties)

This is the definition file used to specify the settings required for event action.

For details, see the *1.5.3 Setting event actions*.

1.4.4 Mail template definition file

This is the definition file used to specify the settings required for other products linkage.

For details, see the *4.5 Linkage with JP1/Service Support* or *4.6 Linkage with JP1/Navigation Platform*.

1.4.5 Command template definition file

This is the definition file used to specify the settings required for other products linkage.

For details, see the *4.7.3 Format of command definition files*.

1.5 Setup

This section describes the following:

- Creating, editing, and deleting resource assignment rules, changing priorities for the rules, and executing assignment rules
- Creating, editing, and deleting user resource assignment rules, changing priorities for the rules, and executing assignment rules
- Setting event actions
- Configuring a virtual machine

For details about the following contents, see the *JP1 Version 11 Integrated Management Getting Started (IT Operations Analytics)*.

- Creating accounts
- Configuring the email server
- Registering management targets
- Creating consumers
- Setting monitoring conditions for management targets

1.5.1 Setting consumers

(1) Creating resource assignment rules

Setting resource assignment rules allows you to automatically register detected virtual machines and hosts to consumers.

Prerequisites:

The consumers to which resources will be assigned have been created.

To do so:

1. Select the **Management** tab, and then select **Setting Consumers** > **Resource Assignment Rules** from the left pane.
2. To create assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To create assignment rules for hosts, select the **Assignment Rules for Hosts** tab.
3. Click the **Create Rules** button.
4. Fill in **Rule Name** and **Description**.
5. Fill in **Conditions**.

   Attributes:

   For assignment rules for virtual machines: Select **Virtual Machine** or **Cluster Name**.

   For assignment rules for hosts: Select **Host Name** or **OS Type**.

   Conditions:

   Select **Equal to**, **Begins with**, **Ends with**, or **Includes**.

Value:

Enter a condition value.

6. Select the assignment-destination consumer in **Assignment Destination**.
7. Click the **OK** button.

(2) Editing resource assignment rules

You can edit created resource assignment rules.

To do so:

1. Select the **Management** tab, and then select **Setting Consumers** > **Resource Assignment Rules** from the left pane.
2. To edit assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To edit assignment rules for hosts, select the **Assignment Rules for Hosts** tab.
3. Select the check box of the rule you want to edit from the **List of Rules**, and then click the **Edit Rules** button.
4. Edit **Rule Name**, **Description**, **Conditions**, and **Assignment Destination**.
5. Click the **OK** button.

Virtual machines and hosts that are detected after the above operation has been completed are assigned to consumers according to the rules after the edit. Virtual machines and hosts that have already been assigned to consumers are not reassigned. You will need to assign such virtual machines and hosts manually, as necessary.

(3) Deleting resource assignment rules

You can delete unnecessary resource assignment rules.

To do so:

1. Select the **Management** tab, and then select **Setting Consumers** > **Resource Assignment Rules** from the left pane.
2. To delete assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To delete assignment rules for hosts, select the **Assignment Rules for Hosts** tab.
3. Select the check box of the rule you want to delete from the **List of Rules**, and then click the **Delete Rules** button.
4. The Delete Assignment Rules dialog box appears. Confirm that the assignment rule you want to delete is displayed in the dialog box.
5. Click the **OK** button.

(4) Changing priorities

You can change priorities among assignment rules for multiple resources.

To do so:

1. Select the **Management** tab, and then select **Setting Consumers** > **Resource Assignment Rules** from the left pane.
2. To change the priority among assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To change the priority among assignment rules for hosts, select the **Assignment Rules for Hosts** tab.
3. Click the **Change Priority** button.
4. In the Change Priority for Rules dialog box, select the rule for which you want to change the priority, and then click the **Up** or **Down** button.
5. After you finish editing the priority, click the **OK** button.

(5) Executing assignment rules

You can execute resource assignment rules for unassigned virtual machines or hosts to assign them to consumers.

To do so:

1. Select the **Management** tab, and then select **Setting Consumers** > **Resource Assignment Rules** from the left pane.
2. To execute assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To execute assignment rules for hosts, select the **Assignment Rules for Hosts** tab.
3. To execute assignment rules for virtual machines, click the **Assign Virtual Machines** button. To execute assignment rules for hosts, click the **Assign Hosts** button.
4. To execute assignment rules for virtual machines, the Assign Virtual Machines dialog box appears. When executing assignment rules for hosts, the Assign Hosts dialog box appears. In the displayed dialog box, click the **OK** button.

1.5.2 Configuring monitoring

(1) Creating user resource assignment rules

Setting user resource assignment rules allows you to automatically register detected virtual machines, Windows hosts, and Linux/UNIX hosts to user resource threshold profiles.

Prerequisites:

The threshold profiles to which resources will be assigned have been created.

To do so:

1. Select the **Management** tab, and then select **Monitoring Configuration** > **User Resource Assignment Rules** from the left pane.
2. To create assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To create assignment rules for Windows hosts, select the **Assignment Rules for Windows** tab. To create assignment rules for Linux/UNIX hosts, select the **Assignment Rules for Linux/UNIX** tab.

3. Click the **Create Rules** button.
4. Fill in **Rule Name** and **Description**.
5. Fill in **Conditions**.

   Attributes:

   For assignment rules for virtual machines: Select **Virtual Machine**, **Cluster Name**, or **Consumer Name**.

   For assignment rules for Windows hosts: Select **Host Name** or **Consumer Name**.

   For assignment rules for Linux/UNIX hosts: Select **Host Name** or **Consumer Name**.

   Conditions:

   Select **Equal to**, **Begins with**, **Ends with**, or **Includes**.

   Value:

   Enter a condition value.
6. Select the assignment-destination user resource threshold profile in **Assignment Destination**
7. Click the **OK** button.

(2) Editing user resource assignment rules

You can edit created user resource assignment rules.

To do so:

1. Select the **Management** tab, and then select **Monitoring Configuration** > **User Resource Assignment Rules** from the left pane.
2. To edit assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To edit assignment rules for Windows hosts, select the **Assignment Rules for Windows** tab. To edit assignment rules for Linux/UNIX hosts, select the **Assignment Rules for Linux/UNIX** tab.
3. Click the **Create Rules** button.
4. Edit **Rule Name**, **Description**, **Conditions**, and **Assignment Destination**.
5. Click the **OK** button.

Virtual machines, Windows hosts, and Linux/UNIX hosts that are detected after the above operation has been done are assigned to user resource threshold profiles according to the rules after the edit. Virtual machines, Windows hosts, and Linux/UNIX hosts that have already been assigned to user resource threshold profiles are not reassigned. You will need to assign such virtual machines, Windows hosts, and Linux/UNIX hosts manually as necessary.

(3) Deleting user resource assignment rules

You can delete unnecessary user resource assignment rules.

To do so:

1. Select the **Management** tab, and then select **Monitoring Configuration** > **User Resource Assignment Rules** from the left pane.
2. To edit assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To edit

assignment rules for Windows hosts, select the **Assignment Rules for Windows** tab. To edit assignment rules for Linux/UNIX hosts, select the **Assignment Rules for Linux/UNIX** tab.

3. Select the check box of the rule you want to delete from the **List of Rules**, and then click the **Delete Rules** button.
4. When executing assignment rules for virtual machines, the Delete Assignment Rules for Virtual Machines dialog box appears. When executing assignment rules for Windows hosts, the Delete Assignment Rules for Windows dialog box appears. When executing assignment rules for Linux/UNIX hosts, the Delete Assignment Rules for Linux/UNIX dialog box appears. Confirm that the assignment rule you want to delete is displayed in the dialog box.
5. Click the **OK** button.

(4) Changing priorities

You can change priorities among assignment rules for multiple user resources.

To do so:

1. Select the **Management** tab, and then select **Monitoring Configuration** > **User Resource Assignment Rules** from the left pane.
2. To change the priority among assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To change the priority among assignment rules for Windows hosts, select the **Assignment Rules for Windows** tab. To change the priority among assignment rules for Linux/UNIX hosts, select the **Assignment Rules for Linux/UNIX** tab.
3. Click the **Change Priority** button.
4. In the Change Priority for Rules dialog box, select the rule for which you want to change the priority, and then click the **Up** or **Down** button.
5. After you finish editing the priority, click the **OK** button.

(5) Executing assignment rules

For virtual machines, Windows hosts, or Linux/UNIX hosts you can execute user resource assignment rules that have not been assigned to consumers to assign them to user resource threshold profiles.

To do so:

1. Select the **Management** tab, and then select **Monitoring Configuration** > **User Resource Assignment Rules** from the left pane.
2. To execute assignment rules for virtual machines, select the **Assignment Rules for Virtual Machines** tab. To execute assignment rules for Windows hosts, select the **Assignment Rules for Windows** tab. To execute assignment rules for Linux/UNIX hosts, select the **Assignment Rules for Linux/UNIX** tab.
3. To execute assignment rules for virtual machines, click the **Assign Virtual Machines** button. To execute assignment rules for Windows hosts, click the **Assign Windows Hosts** button. To execute assignment rules for Linux/UNIX hosts, click the **Assign Linux/UNIX Hosts** button.

4. When executing assignment rules for virtual machines, the Assign Virtual Machines dialog box appears. When executing assignment rules for Windows hosts, the Assign Windows Hosts dialog box appears. When executing assignment rules for Linux/UNIX hosts, the Assign Linux/UNIX Hosts dialog box appears. In the displayed dialog box, click the **OK** button.

1.5.3 Setting event actions

Setting event actions allows you to execute a batch file for event action execution when a JP1/OA event is registered. You can enable automatic notifications when an error is detected by JP1/OA by defining commands to be executed when an event is registered in the event action execution file.

(1) Defining a batch file for event action execution

Create a batch file for event action execution and define commands to be executed when an event is registered in the batch file. You can specify any value for the file name, but the extension must be .bat.

In the event action execution file, you can see information about the event that triggered an event action through environment variables. The following table shows the environment variables that can be specified in a batch file for event action execution.

Table 1-3 List of environment variables that can be specified in a batch file for event action execution

Variable name	Description
ANALYTICS_SOURCE	Device name
ANALYTICS_DEVICE	Device type
ANALYTICS_DESCRIPTION	Message
ANALYTICS_CATEGORY	Category
ANALYTICS_SEVERITY	Level
ANALYTICS_DATE	Registration date
ANALYTICS_STATE	Status
ANALYTICS_EVENTID	Event ID
ANALYTICS_GROUPS	Group name
ANALYTICS_NODEID	Node ID
ANALYTICS_COMPONENTID	Component ID
ANALYTICS_PERFCOMPONENTID	Performance
ANALYTICS_NAME	Name of a host where JP1/OA is running

(2) Editing the event action definition file

Edit the event action definition file to specify the name of a batch file for event action execution, the maximum number of event actions that can be executed simultaneously, and the time-out time.

1. Edit the event action definition file.

Edit the event action definition file. The event action definition file is located as follows:

Storage folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf

For cluster systems:

shared-folder-name\Analytics\conf

File name: EventAction.properties

The event action definition file must be saved in UTF-8 file format. When you save the file, prevent a BOM (byte order mark) from being added to the file.

Definition example when a batch file for event action execution is `C:\Program Files\sample\EventActionSample.bat`, the maximum number of event actions that can be executed simultaneously is 10, and the time-out time is 5 minutes

```
EventAction.cmd=C:\\Program Files\\sample\\EventActionSample.bat
EventAction.maxCount=10
EventAction.timeOut=300000
```

If five minutes or more have elapsed since the definition file was last loaded, JP1/OA reloads the definition file before running an event action.

(3) Format of the event action definition file

The event action definition file is a definition file for configuring event actions.

Format

Specification key name=setting-value

File

EventAction.properties

When you save a file, use UTF-8 for the character code of the file and prevent a BOM (byte order mark) from being added to the file.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf

For cluster systems:

shared-folder-name\Analytics\conf

Timing of definition application

JP1/OA regularly monitors (at intervals of 5 minutes) the event action definition file. If the file is updated, the changes are automatically applied.

Details of description

Specify a specification key name and its setting value by entering a pair in each line. When you create the event action definition file, note the following points:

- Lines beginning with a hash marks (#) are treated as comment lines.
- Blank lines are ignored.
- The setting values are case-sensitive.
- If the setting value is invalid, the default value is set.
- If you specify the same specification key several times in the file, the last specified key is used.
- To specify a tab, specify "\t".
- To display a backslash (\), specify "\\".
- If you want to set "’", specify "\’".
- If you want to display "”", specify "\”".
- Only an absolute path can be specified. A path specified in an environment variable cannot be set for the path.

Setting elements

Table 1-4 Setting elements of the event action definition file

Key name	Settings	Settable value	Default value
EventAction.cmd	Specifies a batch file in absolute path for event action execution	ASCII characters Characters within 260 bytes, excluding control characters - Spaces are excluded.	Null
EventAction.maxCount	Specifies the maximum number of event actions that can be executed simultaneously	Characters within 255 bytes, excluding control characters	10
EventAction.timeOut	Specifies the time-out time for event actions(in milliseconds).	Characters within 255 bytes, excluding control characters	300000

1.5.4 Configuring a virtual machine

Depending on the conditions under which virtual machines are configured, you might be able to obtain the host name from a virtual machine on which the managed applications are running. The conditions vary depending on the

virtualization software.

(1) For VMware

- VMware Tools is installed on the guest OS.

(2) For Hyper-V

- The guest OS is a Windows OS.
- Data exchange on the virtual machine is enabled by clicking **Management**, **Integration Services**, and **Data Exchange**.
- The Hyper-V Data Exchange service is running on the guest OS.
- The Hyper-V Virtual Machine Management service is running on the guest OS.
- The Hyper-V integrated service is installed on the guest OS.

2.Administration

2.1 Outputting resource information

In JP1/OA, you can output information for a managed resource to an HTML or CSV file. You can use this information to create materials such as failure reports.

For details about the specification of the CSV file, see *Appendix F. Format for Output of Resource Information to CSV Files*.

2.1.1 Outputting information from the E2E View window

From the **E2E View** window, the relation information between resources displayed in the window can be output to an HTML file while keeping the window image as is.

In addition, the following information can be output to a CSV file:

- Basic information for the base point resource (the resource specified for analysis) and the list of its related resources
- Performance information for the base point resource (the most recent values)

From the detailed window for the resource, you can output to a CSV file the following items of information that are related to the selected resource:

- Basic information
- Performance information for the selected metric (in chronological order)
- List of events

  Only the events that are displayed in the window are output. If the list continues over multiple pages, output the CSV file for each page. The filter that is applied to the list is also applied to the output result.

2.1.2 Outputting information from the Event Analysis View window

From the **Event Analysis View** window, the event information and performance information that is displayed in the window can be output to an HTML file while keeping the window image as is.

2.1.3 Outputting information from the Performance Analysis View window

From the **Performance Analysis View** window, the resource configuration and performance information that is displayed in the window can be output to an HTML file while keeping the window image as is.

In addition, the following items of information that are related to the resource under detailed analysis can be output to a CSV file:

- Performance information for the metric that is displayed in the **Detailed Analysis Area** area (in chronological order)

2.1.4 Outputting information from the Analyze Bottleneck window

From the **Analyze Bottleneck** window, the bottleneck analysis information displayed in the window can be output to

an HTML file while keeping the window image as is.

In addition, the following items of information that are related to the resource under analysis can be output to a CSV file:

- Performance information for the metric that is displayed in the chart (in chronological order)
- A list of configuration change events

  The filter that is applied to the list is also applied to the output result. The period specified by using **Time period for graph** or selected inside the chart is also applied to the output result.

The following table shows information that can be output from the **Analyze Bottleneck** window.

Table 2-1 Information that can be output from the Analyze Bottleneck window

Information that can be output	Window name			
	Verify Bottleneck	**Check Impact**	**Check Noisy Neighbor**	**Check Related Changes**
Window image	Y	Y	Y	Y
Performance information (in chronological order)	Y	N	Y	Y
Configuration change events	N	N	N	Y

(Legend) Y: Can be output N: Cannot be output

Note: There is no information that can be output from the **Summary** and the **Check Recovery Plan** windows.

2.1.5 Outputting information from the Event window

From the **All Events** tab in the **Event** window, the list of events can be output to a CSV file.

Only the events that are displayed in the window are output. If the list continues over multiple pages, output the CSV file for each page. The filter that is applied to the list is also applied to the output result.

2.2 Importing resource information to the Performance Analysis View window

You can import JP1/PFM reports and performance information managed by other software. The imported information can then be displayed in the **Performance Analysis View** window and used for correlation analysis.

In the **Performance Analysis View** window, click the **Import External Graph Data** button to import resource information.

The following types of files can be imported:

- CSV files to which JP1/PFM reports were output
- Files that contain output performance information, where information items are separated by tabs (TSV option)

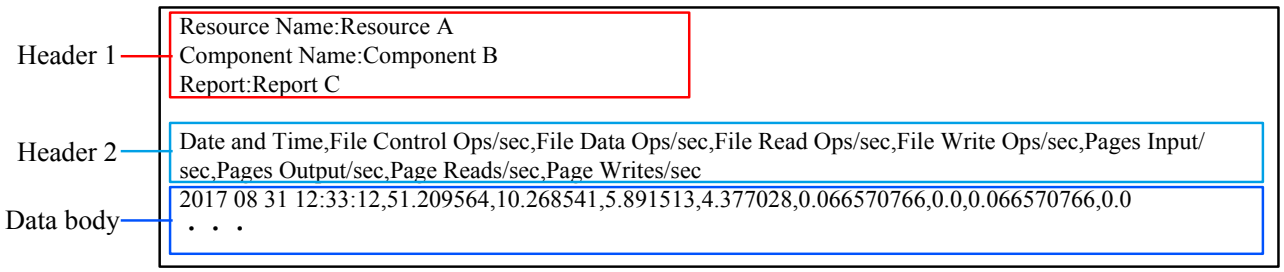
Note that the maximum size of the files is 1 MB.

The following character encodings can be used: UTF-8, US-ASCII, windows-1252, ISO-8859-1, UTF-16, UTF-16BE, UTF-16LE, Shift-JIS, EUC-JP, EUC-JP-LINUX, and MS923.

2.2.1 Configuration of input files

Input files consist of the following elements:

- Header 1
- Header 2
- Data body



Note the following when editing the input file:

- The maximum number of data series that can be displayed in a single graph is 32. If the number exceeds 32, reduce the number of rows or split the file into multiple files when importing the file.

Header 1

- Header 1 is optional. Omitting header 1 entirely will not result in an error.
- A line break is treated as a delimiter between input lines.
- In each line, if you specify a value that includes a colon (`:`), the colon and any text after the colon will be ignored.

Data body

- You must enter a line break after the last line of data.
- The performances values displayed in performance graphs in the **Performance Analysis View** window are approximations of the performance values that are specified in the input file and that have been processed as floating-point type data. If a specified performance value is seven digits or fewer, the specified value will be displayed.

2.2.2 Format of a CSV file to which a JP1/PFM report was output

You can import reports output from JP1/PFM in CSV format (information items are delimited by commas).

(1) Format of header 1

The following table describes the parts that make up header 1.

Input line	Location to which the definition is applied
Resource Name: *resource-name*#1	Value in the **Agent Host** column of the legend displayed on the right of the performance graph
Component Name: *component-name*#1	Value in the **Agent Instance** column of the legend displayed on the right of the performance graph
Report: *report-name*#2	At the beginning of the performance graph title

#1: For historical reports (for multiple Agents), you do not need to specify this line. If you specify this line, it will be ignored.

#2: If you omit this line, only the input file name will be displayed as the performance graph title.

(2) Format of header 2 and the data body

Note the following points when editing the input file.

- "Date and Time" and "Record Time" must be specified in either of the following formats. If these items are specified in a different format, change the date format specified in JP1/PFM, or edit the CSV file directly.

  YYYY MM DD hh:mm:ss

  YYYY/MM/DD hh:mm:ss
- If both "Date and Time" and "Record Time" are specified, "Date and Time" takes priority.

(3) Example

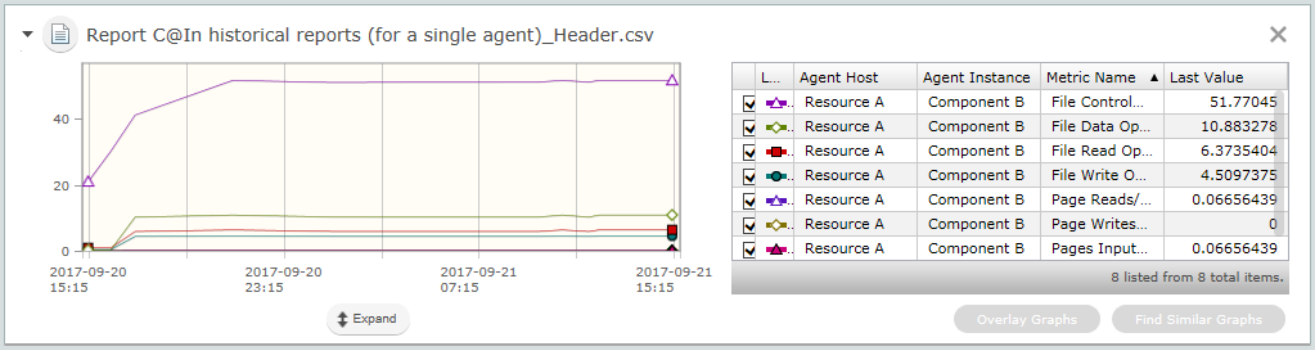
The following is an example of a CSV file to which header 1 has been added:

File name: "In historical reports (for a single agent)_Header.csv"

```
Resource Name:Resource A
Component Name:Component B
Report:Report C

Date and Time,File Control Ops/sec,File Data Ops/sec,File Read Ops/sec,File Write Ops/sec,Pages
Input/sec,Pages Output/sec,Page Reads/sec,Page Writes/sec
2017 09 20 13:10:12,5.209564,0.268541,0.891513,0.377028,0.000570766,0.0,0.000570766,0.0
2017 09 20 14:10:11,10.209564,0.268541,0.891513,0.377028,0.000570766,0.0,0.000570766,0.0
2017 09 20 15:10:10,20.209564,0.268541,0.891513,0.377028,0.000570766,0.0,0.000570766,0.0
2017 09 20 16:10:12,30.209564,0.268541,0.891513,0.377028,0.000570766,0.0,0.000570766,0.0
2017 09 20 17:10:12,41.25039,10.266719,5.890467,4.376251,0.06655895,0.0,0.06655895,0.0
:
```

The following is the graph displayed by importing the above CSV file:



2.2.3 Format of a file containing output performance information, separated by tabs

You can import performance information output from another software program by creating a tab-separated file based on the output information.

(1) Format of header 1

The following table describes the parts that make up header 1.

Input line	Location to which the definition is applied
Resource Name: *resource-name*	Value in the **Resouce Name** column of the legend displayed on the right of the performance graph
Component Name: *component-name*	Value in the **Component Name** column of the legend displayed on the right of the performance graph
Report: *report-name*#	At the beginning of the performance graph title

#: If you omit this line, only the input file name will be displayed as the performance graph title.

(2) Format of header 2 and the data body

The following table describes the parts that make up header 2 and the data body.

Column in header 2	Setting	Setting value in the data body
Date and Time	Date	Values must be specified in either of the following formats. You cannot specify multiple values that have the same date. *YYYY MM DD hh:mm:ss* *YYYY/MM/DD hh:mm:ss*
Items other than" "Date and Time"	Performance value	Numerical values

Note 1: You must specify header 2 and the data body. If you omit a row or a column, an error occurs.

Note 2: Values specified for items other than "Date and Time" will be used as values in the **Metric Name** column in the legend.

(3) Example

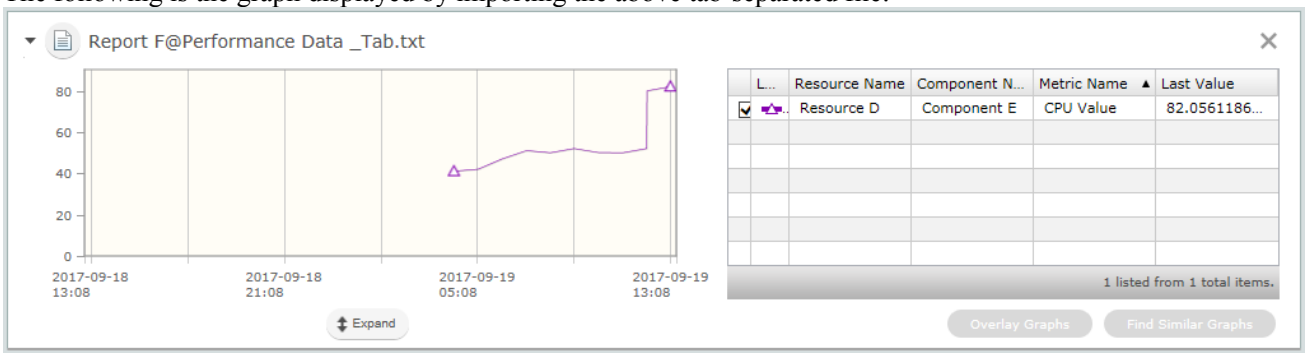
The following is an example of a tab-separated file to which header 1 has been added:

```
Resource Name:Resource D
Component Name:Component E
Report:Report F

Date and Time        CPU Value
2017/09/19 04:11:00          41.0769
2017/09/19 05:11:00          42.0769
2017/09/19 06:11:00          47.0769
2017/09/19 07:11:00          51.0769
2017/09/19 08:10:00          50.0034
:
```

File name: "Performance Data _Tab.txt"

The following is the graph displayed by importing the above tab-separated file:



2.3 Maintenance

2.3.1 Backing up data in a JP1/OA system (non-cluster configuration)

Back up the configuration information and database information of JP1/OA before you perform tasks such as migrating JP1/OA to a new host or performing database maintenance.

Important note:
Make sure that sufficient free space is available on the disk on which the folder for backup files is located. As a guideline, prepare 5 GB of free space in addition to the size (#) of the backup files.

(#) Size of files in *JP1/OA-installation-directory*`\data\database`
When products that use Common Component coexist, you must add the size required for backup of those products.

Who can perform this task:

Users who have Administrator permissions for the OS

Tip:
When you back up the configuration information about JP1/OA or database information, if you can exclude the user information that is managed by Common Component from the backup targets, you might not need to stop and start the service. For details, see *7.8.1 backupsystem (backs up the JP1/OA system).*

To back up a JP1/OA system (non-cluster configuration):

1. Shut down the JP1/OA system by executing the `hcmds64srv` command with the stop option specified.
2. Execute the `backupsystem` command to back up the database and configuration information for JP1/OA.
3. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA system.

Data is backed up to the specified backup folder.

Tip:
The files below are not backed up by the `backupsystem` command. Back them up manually if necessary:
• SSL server certificate file for HTTPS connection
• Private key file for HTTPS connection

Important note:
If you execute the `hcmds64srv` command with AnalyticsWebService specified for the server option, you can stop and start only the services of the JP1/OA products in the state where the Common Component services have already started. When you start the JP1/OA service in daily operation, omit this option to start all the services.

2.3.2 Backing up data in a JP1/OA system (cluster configuration)

Back up the configuration information and database information of JP1/OA before you perform tasks such as migrating JP1/OA to a new host or performing database maintenance.

Important note:
Make sure that sufficient free space is available on the disk on which the folder for backup files is located. As a guideline, prepare 5 GB of free space in addition to the size (#) of backup files.

(#) Size of files in ***shared-folder-name***\Analytics\data\database
When products that use Common Component coexist, you must add the size required for backup of those products.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

Tip:
When you back up the configuration information about JP1/OA or database information, if you can exclude the user information that is managed by Common Component from the backup targets, you might not need to stop and start the service. For details, see *7.8.1 backupsystem (backs up the JP1/OA system)*.

To back up a JP1/OA system (cluster configuration):

1. Take the following services registered in the cluster software offline:
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
2. Shut down the JP1/OA system by executing the `hcmds64srv` command with the stop option specified.
3. In the cluster software, take the registered HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 services offline.
4. Disable failover of the services registered in the cluster software.
   In the cluster software, set JP1/OA so that it does not restart if resources enter Failed status.
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
5. Execute the `backupsystem` command to back up the database and configuration information for JP1/OA.
6. Enable failover of the services registered in the cluster software and listed below.
   In the cluster software, you can configure JP1/OA to restart resources when they enter Failed status on the current node, and to fail over the resources if they could not be restarted.
   - HAnalytics Engine Database _OA0

- HAnalytics Engine Cluster Database _OA0
- HiRDB/ClusterService _HD1
- HAnalytics Engine
- HAnalytics Engine Web Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- Services of Hitachi Command Suite products
- Services for JP1/Automatic Operation

7. Take the following services registered in the cluster software online:
   - HAnalytics Engine Database _OA0
   - HAnalytics Engine Cluster Database _OA0
   - HiRDB/ClusterService _HD1
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation

   Data is backed up to the specified backup folder.

Tip:
The files below are not backed up by the `backupsystem` command. Back them up manually if necessary:
• SSL server certificate file for HTTPS connection
• Private key file for HTTPS connection

Important note:
If you execute the `hcmds64srv` command with AnalyticsWebService specified for the server option, you can use the server AnalyticsWebService option to stop and start only the services of the JP1/OA products in the state where the Common Component services have already started. When you start the JP1/OA service in daily operation, omit this option to start all the services.

2.3.3 Restoring data in a JP1/OA system (non-cluster configuration)

After performing tasks such as replacing the hosts in a JP1/OA system or performing database maintenance, restore the JP1/OA data that you backed up.

Important note:
• Execute the `backupsystem` command to create the backup data.
• Confirm that the following elements are consistent between the backup host and restoration host:
- Path to the installation destination folder of JP1/OA
- Version, revision, and restricted code of the installed JP1/OA instance (#1)
- Host name (#2)
- IP address
- System locale

#1: You can check the version, revision, and restricted code of JP1/OA in the Version dialog box.
#2: The host name need not be consistent if you are changing the host name of the JP1/OA server or you are restoring the information as part of a migration to an environment with a different host name.

Who can perform this task:

Users who have Administrator permissions for the OS

Tip:
When you restore the configuration information about JP1/OA or database information, if you can exclude the user information that is managed by Common Component from the restoration targets, you might need only to stop and start the JP1/OA service. For details, see *7.8.5 restoresystem (restore the JP1/OA system).*

To restore a JP1/OA system (non-cluster configuration):

1. Shut down the JP1/OA system by executing the `hcmds64srv` command with the stop option specified.
2. Restore the JP1/OA configuration information and database information by executing the `restoresystem` command.

   Tip:
   The files below are not restored by the `restoresystem` command. Relocate them manually if necessary.
   • SSL server certificate file for HTTPS connection
   • Private key file for HTTPS connection

   Store the files for HTTPS connection in the location defined in the user_httpsd.conf file.
3. Reconfigure the following definition files to suit the environment to which the data is being restored.

   These definition files are backed up but not restored.

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

   •Security definition file (security.conf)

   •Port number settings (httpsd.conf, hsso.conf)

   The definition files are stored in the following folders:

   •***backup-folder***`\HBase\base\conf`

   •***backup-folder***`\HBase\base\httpsd.conf`
4. Enable HTTPS connection if it is used for communication between JP1/OA and the Web browser.
5. If you changed the number of the port used for communication between JP1/OA and the Web browser, reset the port number according to the procedure for changing port numbers.
6. Start the JP1/OA system by executing the `hcmds64srv` command with the start option specified.

Data is restored to the specified host.

2.3.4 Restoring data in a JP1/OA system (cluster configuration)

After performing tasks such as replacing a host in a JP1/OA system or performing database maintenance, restore the JP1/OA data you backed up.

Important note:
• Execute the `restoresystem` command on the primary server (the server whose mode is set to online in the cluster.conf file).
• Execute the `backupsystem` command to create backup data.
- Confirm that the following elements are consistent between the backup host and restoration host:
  - Path to the installation destination folder of JP1/OA
  - Version, revision, and restricted code of the installed JP1/OA instance (#1)
  - Host name (#2)
  - IP address
  - System locale

#1: You can check the version, revision, and restricted code of JP1/OA in the Version dialog box.
#2: The host name need not be consistent if you are changing the host name of the JP1/OA server or you are restoring the information as part of a migration to an environment with a different host name.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

Tip:
When you back up the configuration information about JP1/OA or database information, if you can exclude the user information that is managed by Common Component from the backup targets, you might not need to stop and start the service. For details, see *7.8.1 backupsystem (backs up the JP1/OA system) and 7.8.5 restoresystem (restore the JP1/OA system).*

To restore a JP1/OA system (cluster configuration):

1. Make sure that there are no tasks in In Progress, Waiting for Response, Abnormal Detection, or Terminated status.

   If there are such tasks in the system, either stop the tasks, or wait until they enter Completed or Failed status.
2. Take the following services registered in the cluster software offline:
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
3. Shut down the JP1/OA system by executing the `hcmds64srv` command with the stop option specified.
4. In the cluster software, take the registered HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 services offline.
5. Disable failover of the services and scripts registered in the cluster software listed below. Configure JP1/OA not to restart if resources enter Failed status in the cluster software.

- HAnalytics Engine Database _OA0
- HAnalytics Engine Cluster Database _OA0
- HiRDB/ClusterService _HD1
- HAnalytics Engine
- HAnalytics Engine Web Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- Services of Hitachi Command Suite products
- Services for JP1/Automatic Operation

6. Bring the shared disk on the active server online.
7. On the primary server, execute the `restoresystem` command to restore the database and configuration information for JP1/OA.

Tip:
The following files are not restored by executing the `restoresystem` command. Relocate them manually if necessary.
• SSL server certificate file for HTTPS connection
• Private key file for HTTPS connection
Store the files for HTTPS connection in the location defined in the user_httpsd.conf file.

8. Shut down the JP1/OA system by executing the `hcmds64srv` command with the stop option specified.
9. On the primary server, reconfigure the following definition files to match the environment to which the data is being restored.

   These definition files are backed up but not restored.

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

   •Security definition file (security.conf)

   •Port number settings (httpsd.conf or user_httpsd.conf)

   The definition files can be found in the following folders:

   •***backup-folder***`\HBase\base\conf`

   •***backup-folder***`\HBase\base\httpsd.conf`

10. If you changed the port number used for communication between JP1/OA and the Web browser on the primary server, make the same changes again in the target environment by following the procedure for changing port numbers.
11. Enable HTTPS connection on the active server if HTTPS connection is used for communication between JP1/OA and the Web browser.
12. Perform steps 8 to 11 on the standby server.
13. Enable failover of the services and scripts listed below registered in the cluster software.

    Configure the cluster software to restart resources on the current node if they enter Failed status, and to fail over the applicable resources if they could not be restarted.

    - HAnalytics Engine Database _OA0

- HAnalytics Engine Cluster Database _OA0
- HiRDB/ClusterService _HD1
- HAnalytics Engine
- HAnalytics Engine Web Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- Services of Hitachi Command Suite products
- Services for JP1/Automatic Operation

14. Bring the following services and scripts registered in the cluster software online:
    - HAnalytics Engine Database _OA0
    - HAnalytics Engine Cluster Database _OA0
    - HiRDB/ClusterService _HD1
    - HAnalytics Engine
    - HAnalytics Engine Web Service
    - HBase 64 Storage Mgmt Web Service
    - HBase 64 Storage Mgmt SSO Service
    - HBase 64 Storage Mgmt Web SSO Service
    - Services of Hitachi Command Suite products
    - Services for JP1/Automatic Operation

    Data is restored to the specified host.

2.3.5 Starting a JP1/OA system (non-cluster configuration)

This section describes how to start a JP1/OA system by using the `hcmds64srv` command. Do not use Service Control Manager to start a system. If you use Service Control Manager, the system might fail to start.

Who can perform this task:

Users who have Administrator permissions for the OS

To start a JP1/OA system (non-cluster configuration):

From the command prompt, execute the `hcmdssrv` command with the start option specified.

Important note:
If you execute the `hcmds64srv` command with AnalyticsWebService specified for the server option, you can use the server AnalyticsWebService option to stop and start only the services of the JP1/OA products in the state where the Common Component services have already started. When starting JP1/OA in the course of day-to-day operation, start all services with this option omitted.

2.3.6 Starting a JP1/OA system (cluster configuration)

This section describes how to start a JP1/OA system by performing operations from the cluster software. Bring services registered in the cluster software online within the software. Do not start the services directly.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To start a JP1/OA system (cluster configuration):

In Failover Cluster Manager, right-click the resource group that contains the JP1/OA service, and click **Bring this service or application online**.

The JP1/OA system starts.

2.3.7 Stopping a JP1/OA system (non-cluster configuration)

This section describes how to stop a JP1/OA system by using the `hcmds64srv` command. Do not use Service Control Manager to stop the services. If you use Service Control Manager, the services might fail to stop.

Who can perform this task:

Users who have Administrator permissions for the OS

To stop a JP1/OA system (non-cluster configuration):

From the command prompt, execute the `hcmds64srv` command with the stop option and the server option specified.

The JP1/OA system stops.

Important note:
If you execute the `hcmds64srv` command with AnalyticsWebService specified for the server option, you can use the server AnalyticsWebService option to stop and start only the services of the JP1/OA products in the state where the Common Component services have already started. When stopping JP1/OA in the course of day-to-day operation, stop all services with this option omitted.

2.3.8 Stopping a JP1/OA system (cluster configuration)

This section describes how to stop a JP1/OA system by performing operations from the cluster software. Take the services registered in the cluster software offline within the cluster software. Do not stop the services directly.

Who can perform this task:

Domain user with Administrator permissions for the OS and administration permission for the cluster

To stop a JP1/OA system (cluster configuration):

1. Bring the following services and scripts registered in the cluster software online:
   - HAnalytics Engine Database _OA0
   - HAnalytics Engine Cluster Database _OA0
   - HiRDB/ClusterService _HD1
   - HAnalytics Engine
   - HAnalytics Engine Web Service

- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- Services of Hitachi Command Suite products
- Services for JP1/Automatic Operation

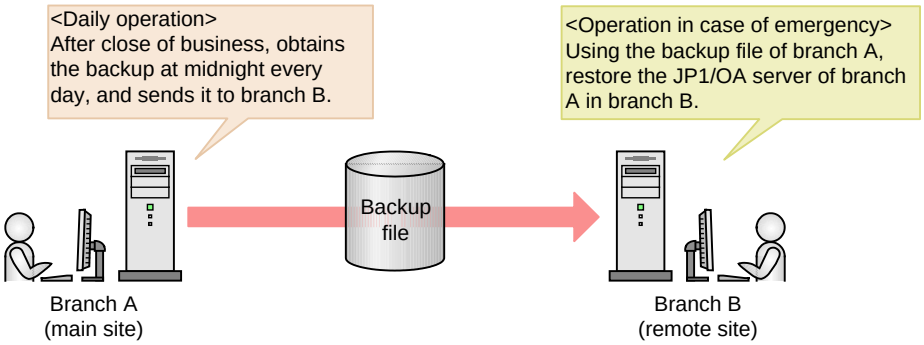
The JP1/OA system is now stopped.

2.3.9 Restoring JP1/OA servers remotely by using backup files

You can restore JP1/OA servers remotely by using backup files, even if a JP1/OA server stops for any reason. You can use this method for disaster recovery when a large disaster or system failure occurs.

See the following figure for details.

Figure 2-1 Example of restoring a JP1/OA server remotely by using backup files



Branch A, which is the main site, obtains the backup file after close of business at midnight every day, and sends it to branch B, which is a remote site. Branch B always retains the backup file of branch A created at midnight on the previous day. Because of this, if a disaster occurs in branch A and its JP1/OA server stops, the JP1/OA server can be restored in branch B from the backup file created at midnight on the previous day.

The procedure for restoring the JP1/OA server remotely by using the backup file is described below.

Prerequisite conditions

The following items must match between the JP1/OA server in the main site and the JP1/OA server in the remote site:

- •System locale
- •Versions and revisions of JP1/OA
- •Installation folder of JP1/OA
- •If Hitachi Command Suite products are installed, the environment of the Hitachi Command Suite products (configuration, versions, revisions, and limited code)
- •If JP1/Automatic Operation is installed, the environment for JP1/Automatic Operation (configuration, version, revisions, and limited code)

Flow of restoring JP1/OA servers remotely by using the back-up file:

The following figure explains the flow for restoring the JP1/OA server in a remote site by using the backup file of

the main site.

Table 2-1 Flow of restoring JP1/OA servers remotely by using the backup file

Timing	Main site	Remote site
During normal operation	Backs up data. (#)	--
	Sends the backed up file to a remote site.	--
When a disaster or failure occurs	--	Uses the latest backup file to restore the JP1/OA server in the main site.

(Legend)--: Not applicable

We recommend you back up data regularly and automatically.

Procedure during normal operation:

Obtain the latest backup file of the main site, and send it to a remote site.

1. Obtain the latest backup file of the main site.

For details about how to obtain the backup file of JP1/OA servers, see *2.3.1 Backing up data in a JP1/OA system (non-cluster configuration)*.

2. Send the obtained backup file of the main site to a remote site.

Tip:
You cannot back up the files below by the `backupsystem` command. If you intend to use the same file in the main site and a remote site, back up data manually when necessary, and send it to the remote site.
• SSL server certificate file for HTTPS connection
• Private key file for HTTPS connection

You can use different files in the main site and a remote site. In that case, back up or create the above files separately in the main site and the remote site.

Procedure when a disaster or failure occurs:

Use the latest backup file of the main site in the remote site to restore the JP1/OA server in the main site.

1. When the JP1/OA system is running, execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA system.
2. Execute the `restoresystem` command to restore settings or database information of JP1/OA in the main site.

Tip:
You cannot restore the files below by using the `restoresystem` command. If you intend to use the same file in the main site and a remote site, reallocate it manually when necessary.
• SSL server certificate file for HTTPS connection
• Private key file for HTTPS connection
Store the files for HTTPS connection in the location defined in the user_httpsd.conf file.

3. Reset the definition files below according to the remote site environment.

You can back up the following definition files by using the `backupsystem` command, but cannot restore by using the `restoresystem` command.

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

•Security definition file (security.conf)

•Port number settings (httpsd.conf, hsso.conf)

•HTTPS connection settings (httpsd.conf)

The definition files are stored in the following folders:

•***backup-destination-folder***`\HBase\base\conf`

•***backup-destination-folder***`\HBase\base\httpsd.conf`

4. Specify HTTPS connection settings if necessary.
5. If you have changed the default port number settings listed below, reset them according to the procedure for changing the port number:

   •Number of the port used for communication between JP1/OA and the Web browser

   •Number of the port used for communication between JP1/OA
6. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA system.

Tip:
If the following settings for the JP1/OA servers in the main site and the remote site are the same, you do not need to perform steps 4 through 6:
•Configuration file for external authentication server linkage (exauth.properties)
•Security definition file (security.conf)
•Port number settings (httpsd.conf, hsso.conf)
•HTTPS connection settings (httpsd.conf)
•Number of the port between JP1/OA and the Web browser
•Number of the port used for communication between JP1/OA and the task-processing engine

7. Execute the `hcmds64chgurl` command to update the URL information according to the remote site environment.

The JP1/OA server of the main site is restored in the remote site.

2.4 Changing the system information

2.4.1 Changing the installation folder of JP1/OA

To change the installation folder of JP1/OA, uninstall JP1/OA and then re-install JP1/OA.

2.4.2 Changing the storage folder of databases

To change the storage folder of databases, uninstall JP1/OA and then re-install JP1/OA.

2.4.3 Extending the retention period for performance information

After JP1/OA is installed, extend the retention period during which performance information can be retained by JP1/OA before or during the operation of JP1/OA. Note that you cannot reduce the retention period.

By default, the retention period for performance information is 4 months. You can only change the retention period from a shorter period to a longer period.

Allowable permissions and roles:

Users that have the Administrator permission of the OS

Prerequisite conditions:

- The folder in which performance information is stored has sufficient free space.

The required space varies depending on the extension of the retention period. Reference the sizing information posted on the JP1 support page, and calculate the required space in advance.

Tip:
Depending on the retention period to expand and the size of the performance information that is already stored, this processing might take some time. Performance information cannot be acquired until the processing ends.

1. Specify the `stop` option for the `hcmds64srv` command, and then execute the command to stop the JP1/OA services.
2. Execute the `backupsystem` command to back up the database and configuration information for JP1/OA.
   For details, see *7.8.1 backupsystem (backs up the JP1/OA system)*.
3. Execute the `expandretention` command to extend the retention period for performance information.
   For details, see *7.8.2 expandretention (extends the retention period for performance information)*.
4. Specify the `start` option for the `hcmds64srv` command, and then execute the command to start the JP1/OA services.
5. If necessary, delete the temporary folder that was created during the execution of the `expandretention` command.

2.4.4 Changing the host name of the JP1/OA server

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. Change the host name of the JP1/OA server.
3. Change the host name specified in ServerName in the user_httpsd.conf file.
   The user_httpsd.conf file is stored in the following folder:

   Common-Component-installation-folder`\uCPSB\httpsd\conf`

4. Restart the JP1/OA server.
5. If the settings to manually start the JP1/OA server are set, you need to execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

2.4.5 Changing the IP address of the JP1/OA server

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. Change the IP address of the JP1/OA server.
3. Restart the JP1/OA server.
4. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

2.4.6 Changing the port number

(1) Changing the port number used between JP1/OA and the web browser

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. To change the port number settings, edit keys in the definition file as follows.
   The port number settings will be different depending on the communication method between JP1/OA and the web browser.

   When the communication method is HTTP:

   - "Listen" in

Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf

Set the new port number "22015" in the following lines:

```
Listen 22015
Listen [::]:22015
#Listen 127.0.0.1:22015
```

Note: Do not change any settings other than the port number.

- "command.http.port" in "command_user.properties" in the following folder

  For non-cluster systems:

  installation-destination-folder-of-JP1/OA\conf

  For cluster systems:

  shared-folder-name\Analytics\conf

  Set the new port number "22015" in the following line:

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

  Note: Do not change any settings other than the port number.

When the communication method is HTTPS:

- "Listen" in

  Common-Component-installation-folder\uCPSB\httpsd\conf\user_httpsd.conf

  Set the new port number "22016" in the following lines:

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

  Note: Do not change any settings other than the port number.

- "command.https.port" in

  installation-destination-folder-of-JP1/OA\command_user.properties

  Set the new port number "22016" in the following line:

```
command.https.port = 22016
```

  Note: Do not change any settings other than the port number.

3. To change the port number settings, edit the shortcut to the program as follows.

In Windows Server 2008:

(1). From the Start menu, select **All Programs** > **JP1_Operations Analytics**, and then open the **Analytics** property.

(2). Change the port number of the URL specified for a link.

In Windows Server 2012:

(1). Display the Start window from the desktop.

(2). Right-click the Start screen, and then click **All Apps**.

(3). Open the **Analytics** property in the JP1_Operations Analytics folder.

(4). Change the port number of the URL specified for a link.

In Windows Server 2016:

(1). Open the Start menu.

(2). Open the **Analytics** property in the JP1_Operations Analytics folder.

(3). Change the port number of the URL specified for a link.

"Execution file of the web browser specified as default" http://localhost:22015/Analytics/

4. Execute the `hcmds64fwcancel` command to register firewall exceptions.
5. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

(2) Changing the port number used between JP1/OA and Common Component

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. To change the port number settings, edit keys in the definition file as follows.
   - "worker.AnalyticsWebService.port" in
     Common-Component-installationfolder`\uCPSB\CC\web\redirector\workers.properties`
     Set the new port number "27100" in the following lines:

worker.AnalyticsWebService.port=27100

   - "webserver.connector.ajp13.port" or "webserver.shutdown.port" in
     Common-Component-installation-folder`\uCPSB\CC\web\containers\AnalyticsWebService\usrconf\usrconf.properties`
     Set the new port number "27100" or "27101" in the following lines:

...
webserver.connector.ajp13.port=27100
...
webserver.shutdown.port=27101
...

     Note: Do not change any settings other than the port number.

3. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

(3) Changing the port number used in the JP1/OA database

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. To change the port number settings, edit keys in the definition file as follows. You might need to edit multiple files, but you do not need to edit files containing port numbers that are not subject to change.
   - "PDNAMEPORT" in
     installation-destination-folder-of-JP1/OA`\system\HDB\CONF\emb\HiRDB.ini`

     Set the new port number "27102" in the following line:

     ```
     PDNAMEPORT=27102
     ```

     Note: Do not change any settings other than the port number.

   - "set pd_name_port" or "set pd_service_port" in
     installation-destination-folder-of-JP1/OA`\system\HDB\CONF\pdsys`

     Set the new port number "27102" or "27103" in the following lines:

     ```
     ...
     set pd_name_port = 27102
     ...
     set pd_service_port = 27103
     ...
     ```

     Note: Do not change any settings other than the port number.

   - "CO.DBPortNo" or "CO.DBRemotePortNo" in "Argus.properties" under the following folder.

     For non-cluster systems:

     installation-destination-folder-of-JP1/OA`\conf`

     For cluster systems:

     shared-folder-name`\Analytics\conf`

     Set the new port number "27102" or "27103" in the following lines:

     ```
     CO.DBPortNo = 27102
     CO.DBRemotePortNo = 27103
     ```

     Note: Do not change any settings other than the port number.

3. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

(4) Changing the port number used between the JP1/OA services

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. To change the port number settings, edit keys in the definition file as follows.
   - "CO.rmi.registoryPort" in "Argus.properties" under the following folder.

     For non-cluster systems:

     installation-destination-folder-of-JP1/OA`\conf`

     For cluster systems:

     shared-folder-name`\Analytics\conf`

     Set the new port number "27104" in the following line:

CO.rmi.registoryPort = 27104

     Note: Do not change any settings other than the port number.

3. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

2.4.7 Changing the port number used between JP1/OA and the SMTP server

Change the port number used between JP1/OA and the SMTP server from the **Email Server Settings** View.

Allowable permissions and roles:

Users that have the Admin permission of JP1/OA

1. Select the **Management** tab, and then select **Notification Configuration** > **Email Server Settings** from the left pane.
2. Click the **Edit Settings** button and enter the new port number in **Port Number**, and then click the **OK** button.

2.4.8 Changing the time settings of the JP1/OA server

(1) Setting the clock of the JP1/OA server forward

Allowable permissions and roles:

Users that have the Administrator permission of the OS

1. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA service.
2. Set the clock of the JP1/OA server forward.
3. Execute the `hcmds64srv` command with the start option specified to start the JP1/OA service.

3.System design

3.1 Consideration of the cluster system

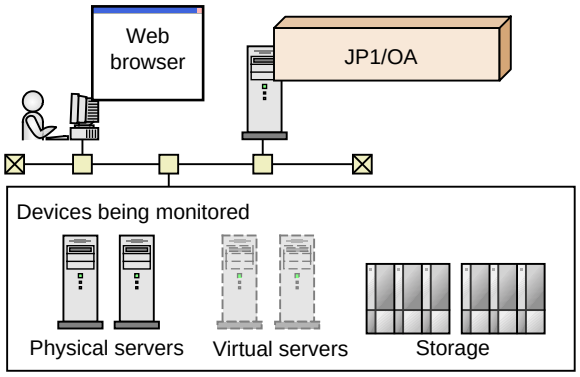
This subsection explains as examples of JP1/OA system configurations a basic system configuration and a cluster configuration.

(1) Basic system configuration

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

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

Figure 3-1 Example configuration for a basic system

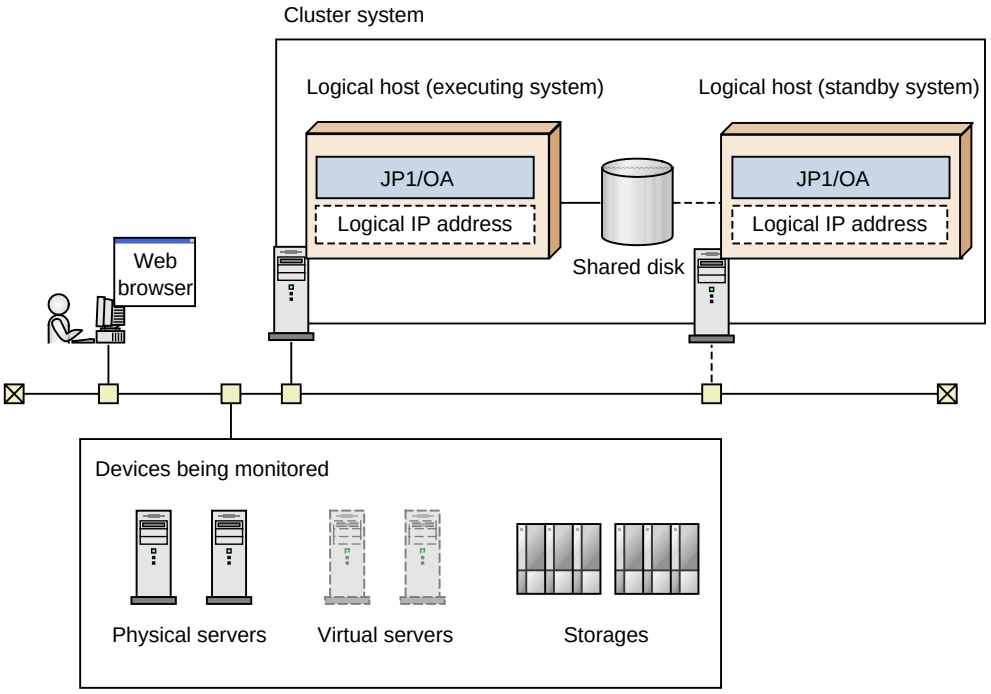


(2) Cluster configuration

JP1/OA supports operation in a cluster system. In a cluster system, if a failure occurs on the executing host that is running JP1/OA, 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/OA use the logical IP addresses stored on the shared disk for communications. When physical servers are swapped due to failover, information about the JP1/OA 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/OA supports only the active-standby cluster configuration.

Figure 3-2 Example configuration for a cluster system



A JP1/OA cluster system has the following characteristics:

- The information stored on the shared disk includes JP1/OA'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/OA.

3.2 Establishing JP1/OA in a cluster system

3.2.1 Procedure for installing JP1/OA in a cluster system

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

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

Table 3-1 Procedure for installing JP1/OA in a cluster system

Task		Required/ optional	Reference
1	Check the installation prerequisites.	Required	3.2.2 Installation prerequisites (for cluster systems)
2	Install JP1/OA.	Required	The reference depends on the current environment and the installation status of the product.(#) For details about the possible environments, see *Table 3-2 Possible environments when setting up a cluster system.*

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

Table 3-2 Possible environments when setting up a cluster system

Current environment	JP1/OA installation status	Common Component installation status	Reference
Cluster system set up	Y	Y	1.1.2 Performing an overwrite installation or an upgrade installation of JP1/OA (in the case of a cluster system)
	N	Y	3.2.4 Installing JP1/OA in a cluster system (if Common Component is already installed in a cluster configuration)
		N	3.2.3 Installing JP1/OA in a cluster system
Cluster system not set up	N	Y	
		N	

(Legend):

Y: installed N: not installed

Note that the following cluster system configurations are excluded from support:

- An instance of JP1/OA currently operating in a non-cluster environment that was migrated into a cluster configuration
- An instance of JP1/OA currently operating in a cluster system environment that was migrated into a single configuration

3.2.2 Installation prerequisites (for cluster systems)

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

- Related Products

If JP1/AO or Hitachi Command Suite is already running in the machine where you want to install JP1/OA, and if the software is running in a non-cluster environment, then it is impossible to operate JP1/OA in a cluster configuration.

- OS and cluster software

The OS must be one of the following:

- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter
- Windows Server 2012 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Standard
- Windows Server 2016 Datacenter
- Windows Server 2016 Standard

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

- The cluster software must be Windows Server Failover Cluster (WSFC).
- Patches and service packs required by JP1/OA and the cluster software must have been applied.

- Configuration

- The environment of each server must be the same so that the same processing can be performed in the event of failover.
- The cluster must be configured with two or more servers.
- Protecting files in file systems that have journal functionality, etc., by preventing them from being deleted due to the system shutting down

- Network

- Communication must be possible by using the IP address that corresponds to the host name (result of execution of the hostname command). It must not be possible for a program such as the cluster software to set a status that disables communication.
- The correspondence between the host name and the IP address cannot be changed while JP1/OA is operating. It must not be possible for programs, such as the cluster software and name server, to change the correspondence.
- The LAN board corresponding to the host name must have the highest priority in the network bind settings. Priority must not be given to any other LAN board, including a heartbeat LAN board.

- DNS operation

- Host names must have been entered without the domain name.

- Shared disk

  To prevent data corruption on the active server in the event of failover, make sure that all the conditions listed below have been met. If the conditions are not met, problems might occur that prevent JP1/OA from working properly, including errors, data loss, and failure to start.

  - JP1/OA must not be installed on the shared disk.
  - A shared disk that can be carried over from the active server to the standby server must be available.
  - The shared disk must have been allocated before JP1/OA was started.
  - Allocation of the shared disk cannot be released during JP1/OA execution.
  - Allocation of the shared disk must be released after JP1/OA has stopped.
  - The shared disk must be locked so that it will not be accessed improperly by multiple servers.
  - Files must be protected by a method such as a journaling file system so that data will not be lost in the event of a system shutdown.
  - The contents of files must be protected and inherited in the event of a failover.
  - Forced failover must be available in the event that the shared disk is being used by a process at the time of a failover.
  - If JP1/OA needs to be started or stopped as part of the recovery process when failure is detected on the shared disk, you must be able to start or stop JP1/OA from the cluster software.

- Logical host name, IP address

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

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

- Port numbers

  The port number for connecting to the Web server must be the same in both the active server and the standby server.

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

3.2.3 Installing JP1/OA in a cluster system

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

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

(1) Tasks required before installation of JP1/OA in a cluster system

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

Before you begin

- Check the installation prerequisites (for cluster system).
- Log in to the JP1/OA server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

(2) Procedure for creating a resource group by using the cluster software

Create a resource group by using the cluster software.

To create a resource group by using the cluster software:

1. Install the cluster software on the active server and the standby server, and then set up the cluster system.

- Install the cluster software according to the procedure specified by the OS.
- Create the cluster by using the cluster software.

2. Create a resource group by using the cluster software. A resource group is a collection of services to be clustered together and treated as a unit for purposes of service failover.

- Register the shared disk used in JP1/OA to the resource group of the cluster software.
- In Windows, register client access points in the resource group of the cluster software.

For the network name, specify the logical host name used in JP1/OA. For the IP address, specify the logical IP.

(3) Installing JP1/OA on the active server and the standby server

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

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

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

   Specify settings as follows:

   - Specify the active server.
   - Specify a drive and folder on the active server as the installation destination. Note that you must specify the drive and folder with the same names as those on the standby server.
   - Specify a path to a local disk for the location of the database.
   - Specify the logical host name of the cluster system.
   - Specify the physical host names of the active server and standby server.

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

   The shared disk does not need to be available on the standby server.
2. Install JP1/OA on the standby server.

   - Specify the standby server.
   - Specify a drive and folder on the standby server as the installation destination. Note that you must specify the drive and folder with the same names as those on the active server.
   - Specify a path to a shared disk for the location of the database.
   - Specify the logical host name of the cluster system.
   - Specify the physical host names of the active server and standby server.

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

(4) Procedure to register services by using the cluster software

Register services by using the cluster software.

To register services by using the cluster software:

1. Move **Current Owner** to the active server by using the cluster software.
2. Register services to the resource group by using the cluster software.

   Set the service dependencies in the order listed below.

   Register services 1 to 8 as service resources.

   1. HAnalytics Engine Database _OA0
   2. HAnalytics Engine Cluster Database _OA0
   3. HiRDB/ClusterService _HD1
   4. HBase 64 Storage Mgmt Web Service
   5. HBase 64 Storage Mgmt SSO Service
   6. HBase 64 Storage Mgmt Web SSO Service
   7. HAnalytics Engine Web Service
   8. HAnalytics Engine

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

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

3.2.4 Installing JP1/OA in a cluster system (if Common Component is already installed in a cluster configuration)

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

(1) Tasks required before installation of JP1/OA in a cluster system

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

Before you begin

- Check the installation prerequisites (for cluster system).
- Log in to the JP1/OA server as a domain user with Administrator permissions on the OS and administrator permissions on the cluster.

(2) Procedure for configuring services before installation (if Common Component is already installed)

Before you install JP1/OA in a cluster system, you must configure services.

To configure services before installation:

1. Use the cluster software to move the resource group where the JP1/AO and the Hitachi Command Suite products are registered to the active server.
2. Use the cluster software to bring the above resource group online.
3. Use the cluster software to bring the JP1/AO and the Hitachi Command Suite services other than HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 offline.
4. Use the cluster software to bring the HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 services offline.
5. Use the cluster software to move the resource group where the JP1/AO and the Hitachi Command Suite products are registered to the standby server.
6. Use the cluster software to bring the above resource group online.
7. Use the cluster software to bring the JP1/AO and the Hitachi Command Suite services other than HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 offline.
8. Use the cluster software to bring the HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 offline.
9. In the cluster software, suppress failover for the resource group where the JP1/AO and the Hitachi Command Suite products are registered.

   Right-click a service in the cluster software, and then select **Properties** and then **Policies**. Then specify the settings so that a restart does not occur if the resource fails. Perform this action for all services registered in the resource group in order to suppress failover.

(3) Installing JP1/OA on the active server and the standby server (if Common Component is already installed)

Install JP1/OA on the active server and standby server.

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

1. Use the cluster software to move the resource group where the JP1/AO and the Hitachi Command Suite products are registered to the active server.
2. Install JP1/OA on the active server.

   Specify settings as follows:

   - Specify the active server.
   - Specify a drive and folder on the active server as the installation destination. Note that you must specify the drive and folder with the same names as those on the standby server.
   - Specify a path to a shared disk for the location of the database.
   - Specify the logical host name of the cluster system.
   - Specify the physical host names of the active server and standby server.

   After installation, if a message is displayed indicating that a restart is required, restart the active server.
3. Use the cluster software to move the resource group where the JP1/AO and the Hitachi Command Suite products are registered to the standby server.
4. Install JP1/OA on the standby server.
   - Specify the standby server.
   - Specify a drive and folder on the standby server as the installation destination. Note that you must specify the drive and folder with the same names as those on the active server.
   - Specify a path to a shared disk for the location of the database.
   - Specify the logical host name of the cluster system.
   - Specify the physical host names of the active server and standby server.

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

(4) Procedure to register services by using the cluster software

Register services by using the cluster software.

To register services by using the cluster software:

1. Use the cluster software to move the resource group where the JP1/AO and the Hitachi Command Suite products are registered to the active server.
2. Use the cluster software to register services in the resource group where the JP1/AO and the Hitachi Command Suite products are registered.

   Set the service dependencies in the order listed below.

   Register services 1 to 8 as service resources.

   1. HAnalytics Engine Database _OA0

2. HAnalytics Engine Cluster Database _OA0
3. HiRDB/ClusterService _HD1
4. HBase 64 Storage Mgmt Web Service
5. HBase 64 Storage Mgmt SSO Service
6. HBase 64 Storage Mgmt Web SSO Service
7. HAnalytics Engine Web Service
8. HAnalytics Engine

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

3. In the cluster software, enable failover for the resource group where the JP1/AO and the Hitachi Command Suite products are registered.

   Right-click a service or script in the cluster software, select **Properties**, and then **Policies**. Then, specify the settings so that a restart can be attempted on the current node if the resource fails and all resources in the target service or application can be failed over if restart fails. Perform this action for all services and scripts registered in the resource group in order to enable failover.
4. Bring the resource group online by using the cluster software.

3.2.5 To change the logical host name or other settings after installation

(1) Changing the configuration of JP1/OA

On the executing node, use a text editor to specify the new logical host name in the "Argus.properties " file located in the ***shared-disk-installation-destination***\conf path as follows:

```
SE.cluster.logicalHostName=logical-host-name
```

(2) Changing the settings of Common Component

1. On the executing and standby nodes, use a text editor to create a cluster settings file. Elements to be specified in the cluster settings file are as follows:

   On the executing node:

   ```
   mode=online
   virtualhost=logical-host-name
   onlinehost=executing-node-host-name
   standbyhost=standby-node-host-name
   ```

   On the standby node:

   ```
   mode=standby
   virtualhost=logical-host-name
   onlinehost=executing-node-host-name
   standbyhost=standby-node-host-name
   ```

   Name the created file "cluster.conf" and store it in ***Common-Component-installation-destination***\Base64\conf.

(3) Applying to JP1/OA the logical host that was changed

Restart the JP1/OA service on the active server and apply the new settings.

To apply the new logical host to the JP1/OA system:

1. Take offline the following services that are registered in the cluster software.
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
2. Execute the `hcmds64srv` command with the stop option specified to stop the JP1/OA system.
3. Take offline the HAnalytics Engine Database _OA0, HAnalytics Engine Cluster Database _OA0 and HiRDB/ClusterService _HD1 services that are registered in the cluster software.
4. Suppress failover of the services below that are registered in the cluster software.
   Specify settings in the cluster software not to restart resources in the failure state.
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
5. Enable failover of the services below that are registered in the cluster software. Specify settings in the cluster software to try to restart resources in the failure state on the current node and to fail over the corresponding resource if the restart fails.
   - HAnalytics Engine Database _OA0
   - HAnalytics Engine Cluster Database _OA0
   - HiRDB/ClusterService _HD1
   - HAnalytics Engine
   - HAnalytics Engine Web Service
   - HBase 64 Storage Mgmt Web Service
   - HBase 64 Storage Mgmt SSO Service
   - HBase 64 Storage Mgmt Web SSO Service
   - Services of Hitachi Command Suite products
   - Services for JP1/Automatic Operation
6. Bring online the following services that are registered in the cluster software.
   - HAnalytics Engine Database _OA0

- HAnalytics Engine Cluster Database _OA0
- HiRDB/ClusterService _HD1
- HAnalytics Engine
- HAnalytics Engine Web Service
- HBase 64 Storage Mgmt Web Service
- HBase 64 Storage Mgmt SSO Service
- HBase 64 Storage Mgmt Web SSO Service
- Services of Hitachi Command Suite products
- Services for JP1/Automatic Operation

The JP1/OA and Common Component services restart, and the new logical host is applied.

Note:
Do not directly stop services that are registered in the cluster software. Take such services offline in the cluster software.

3.2.6 Folders created on the JP1/OA shared disk

When JP1/OA is installed on a cluster system, creates the following folders on the shared disk that is specified.

Table 3-3 Folders created on the shared disk

Product	Application	Created folder
JP1/OA	Folder for definition files	***shared-folder-name***\Analytics\conf
	Log file output folder	***shared-folder-name***\Analytics\logs
	Data folder	***shared-folder-name***\Analytics\data
Common Component	Database installation folder	***shared-folder-name***\HiCommand\database(#)

If Common Component already exists in the cluster environment, a new folder is not created on the shared disk.

4.Linking to other products

4.1 Linkage with the authentication function of JP1/Base

Linkage with the authentication function of JP1/Base allows you to manage users of JP1/OA and perform user authentication by using JP1/Base. To manage users by using JP1/Base, create a JP1 user in the operation window of JP1/Base and configure the JP1 resource group name and permission level. At this time, setting the JP1/OA permission level for the permission level allows the JP1 user to be managed as a JP1/OA user.

Linking with JP1/Base provides the following advantages:

- There is no need to manage users in JP1/OA.
- You can use already existing JP1 users.

When linkage with the authentication function of JP1/Base is enabled and a user who is not registered in JP1/OA logs in to JP1/OA, the user is authenticated by JP1/Base. If a user who is registered in JP1/OA logs in to JP1/OA, JP1/OA manages the authentication and permissions for the user without linkage with JP1/Base.

When linkage with the authentication function of JP1/Base is enabled, the linkage is also effective for users managed by JP1/Automatic Operation and other Hitachi Command Suite products.

This section describes the procedure for linking with the authentication function of JP1/Base.

4.1.1 Setting the external authentication server linkage configuration file

To link with the authentication function of JP1/Base, you must set the external authentication server linkage configuration file.

1. **Open the external authentication server linkage configuration file (exauth.properties).**
   The external authentication server linkage configuration file is stored in the following folder:
   common-component-installation-folder`\conf`

2. **Specify "jp1base" for the value of the auth.server.type specification key.**

3. **Overwrite the external authentication server linkage configuration file.**

4. **Restart JP1/OA to apply the definition file.**
   Execute the `hcmds64srv` command with the stop option specified to stop JP1/OA.
   Execute the `hcmds64srv` command with the start option specified to start JP1/OA.

4.1.2 Creating and configuring a JP1 user (for linkage with JP1/Base)

Create and configure a JP1 user to manage JP1/OA users by linking with the authentication function of JP1/Base.

1. **Create a user in the operation window of JP1/Base.**

   If there is linkage with JP1/Base, you do not need to register a user in the operation window of JP1/OA.

2. **Specify the JP1 resource group name and permission level in JP1/Base.**

   Define the JP1/Base permission level according to the permission in JP1/OA to link JP1/OA with JP1/Base.

   Create a JP1 resource group with the following permission, and set the permission for the JP1 user.

Table 4-1 Definition of permission level (for linkage with JP1/Base)

Permission in JP1/OA	Permission for JP1/OA specified in JP1/Base
Admin	JP1_Analytics_Admin
Modify	JP1_Analytics_Modify
UserManagement	HCS_UserMng_Admin

For details about the configuration of JP1/Base, see the description about the configuration of user management in the *JP1/Base User's Guide*.

4.1.3 Checking the connection with JP1/Base

After creating and configuring a JP1 user, check whether a connection is established between the user and JP1/Base.

1. **Execute the hcmds64checkauth command.**

   Confirm that the JP1/Base user is correctly authenticated.

4.2 Linkage with a Windows version of a JP1 product

JP1/OA can manage the applications monitored by JP1/IM, JP1/AJS3, and JP1/PFM by linking to these products. When JP1/OA links to the Windows versions of these products, in order to collect application configuration information from each product's server, you must perform either of the following operations before running Management Tool Registration in JP1/OA:

- Enable Windows administrative shares (ADMIN$).
- Create a shared folder.

In addition, if you want to collect JP1 events from JP1/IM, you must enable the following settings:

- The integrated monitoring database
- The event source host mapping function

For details about how to enable these settings, see the *JP1/Integrated Management - Manager Configuration Guide*.

4.2.1 Setting up administrative shares

To enable a Windows administrative share (ADMIN$) in order to link with a Windows version of JP1/IM, JP1/AJS3, or JP1/PFM, configure the registry as is specified in the following table, and then restart the OS.

Table 4-2 Settings to enable Windows administrative shares

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

If you want to register the JP1/OA management software by using a user account without built-in Administrator permissions, you must disable User Account Control (UAC). To disable UAC, configure the registry as is specified in the following table, and then restart the OS.

Table 4-3 Settings to disable User Account Control

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Registry entry	EnableLUA
Value to be set for the registry entry	0 (DWORD)

4.2.2 Configuring a shared folder

To use a shared folder in order in order to link with a Windows version of JP1/IM, JP1/AJS3, or JP1/PFM, perform the following procedure to create a shared folder for each server.

1. Create a folder in any location.

2. Right-click the folder, click **Share** and **Advance Sharing**, and then select the check box for **Share this folder**.

3. Specify a shared name, and then grant access permissions to the same users who have Administrator permissions.

4.3 Linkage with the UNIX version of JP1 products

JP1/OA can manage the applications monitored by JP1/IM, JP1/AJS3, and JP1/PFM by linking to these products. When JP1/OA links to the UNIX version of these products, in order to collect application configuration information from each product's server, you must perform the following operation before running Management Tool Registration in JP1/OA:

- Enable SSH connection on the server.

In addition, if you want to collect JP1 events from JP1/IM, you must enable the following settings.

- The integrated monitoring database
- The event source host mapping function

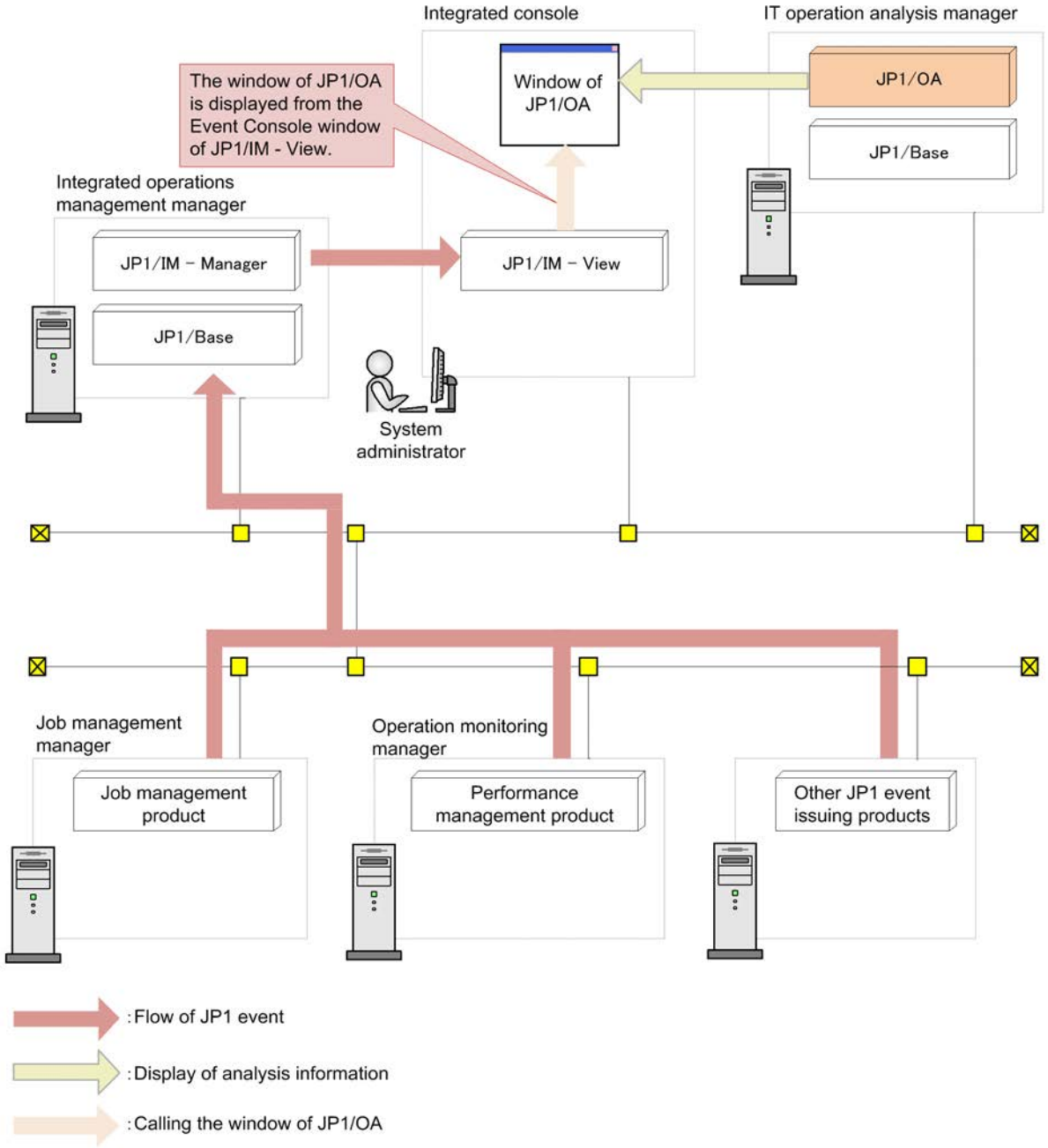
For details about how to enable the settings, see the *JP1/Integrated Management - Manager Configuration Guide*.

4.4 Linkage with JP1/IM

You can configure the operation of the command execution button in JP1/IM - View so that the JP1/OA window is called from JP1/IM - View. This aids identification of the components and users affected by errors reported as JP1 events in the system.

The following figure shows an example of IT operation analysis by linking JP1/OA with JP1/IM.

Figure 4-1 Example of IT operation analysis by linking JP1/OA with JP1/IM



The window of JP1/OA to be called by JP1/IM is the Search Resources window.

In the Search Resources window, you can see the results obtained from searching by setting JP1 event information as search keywords.

The window of JP1/OA to be called by JP1/IM does not support single sign-ons.
When the login window appears at the call of the window of JP1/OA, the window which JP1/IM calls appears after login.

This section describes the procedure for linking JP1/OA with JP1/IM.

4.4.1 Configuring the command execution button of JP1/IM - View

Set the operation to call the window of JP1/OA from JP1/IM - View for the command execution button of JP1/IM - View.

1. Enable the settings of the Command button in JP1/IM - Manager.

Execute the `jcoimdef` command to enable the **Command** button. This operation allows you to execute a client application from the **Command** button of JP1/IM - View.

Example:

```
jcoimdef -i -cmdbtn ON
```

2. Create a command button definition file (cmdbtn.conf).

Set the details of the operation to be executed by the **Command** button of JP1/IM - View in the command button definition file.

Example of starting the search window of JP1/OA by setting the source host name of a JP1 event as a search keyword

```
DESC_VERSION=2
def
# Display the Search Resources window of JP1/OA.
# Pass the source host name of a JP1 event to the execution command.
  btn OAΔ Δ linkage
    cmt Start the Search Resources window of JP1/OA.
    cmdtype client
    inev true
    cmd cmd.exe /K start http://host-name:22015/Analytics/main.htm?module=
analytics^&param[searchType]=servers^&param[searchKey]=${EV"JP1_SOURCEHOST"$URLENC}
  end-btn
end-def
```

Note 1: Write the commands to be executed on a single line.
Note 2: Δ indicates a halfwidth space.

For details about the command button definition file, see the description about the Command button definition file (cmdbtn.conf) in the *JP1/Integrated Management - Manager Command and Definition File Reference*.

For details about specification of inherited information of JP1 events, see the description about the inherited event information at command execution in the *JP1/Integrated Management - Manager Overview and System Design Guide*.

You can set a search keyword for the URL for accessing the Search Resources window of JP1/OA.

For details about parameters that can be specified for URLs, see 5. *Direct Access URL*.

3. Restart JP1/IM - View to apply the definition.

You need to restart JP1/IM - View when configuring the definition of the **Command** button while JP1/IM - View is running.

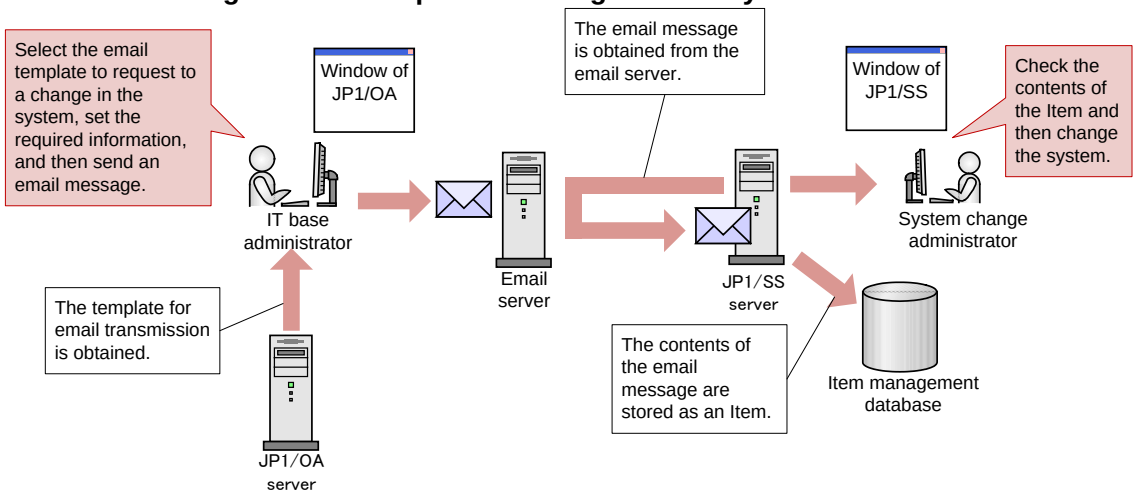
4.5 Linkage with JP1/Service Support

When you manage changes, etc., in the system configuration as Items by JP1/Service Support, Items that inherit resource information managed by JP1/OA can be automatically registered in JP1/Service Support.

Linkage with JP1/Service Support allows JP1/OA to issue, as an Item, an email message in which the resource information is set, and JP1/Service Support to register the received email message.

The following figure shows an example of Item registration by JP1/OA linked with JP1/Service Support.

Figure 4-2 Example of Item registration by JP1/OA linked with JP1/SS



This section describes the procedure for linking JP1/OA with JP1/Service Support.

Preparation

To send email messages from JP1/OA, you must configure the email server for JP1/OA.

To create an Item from an email message in JP1/Service Support, you must configure the settings for registering Items by email for JP1/Service Support.

For details about how to configure the email server for JP1/OA, see the description about the Setting the email server in the *JP1 Version 11 Integrated Management Getting Started (IT Operations Analytics)*.

For details about the settings for creating an Item from an email message in JP1/Service Support, see the description about the Environment settings for registering Items by email in the *JP1/Service Support Configuration and Administration Guide*.

4.5.1 Creating an email template definition file (for linkage with JP1/SS)

Create an email template definition file for registering Items from JP1/OA in JP1/Service Support.

1. Create an email template definition file.

Create an email template definition file. You can specify a desired value for the file name and extension.

The email template definition file must be saved in UTF-8 file format.

Definition example when setting the selected resource name for the subject

```
SE.template.name.string=001_JP1/SS email creation for Item registration
SE.template.description.string=Create email for registering Items in JP1/SS.
SE.mail.template.title.string=Subject: Request to change the structure
(%ANALYTICS_RESOURCENAME%)
SE.mail.template.body.string=Body■Title LFCR<TITLE>Information to be set for the Title element of the
Item</TITLE>LFCR■Summary<SUMMARY>Information to be set for the Summary element of the
Item</SUMMARY>LFCR■Deadline LFCR<DEADLINE>Information to be set for the Deadline element of
the Item</DEADLINE>LFCR■Comments LFCR<FREEDESCRIPTION>Information to be set for the Free
description element of the Item</FREEDESCRIPTION>
SE.mail.template.address.string=xxxxxxx@hitachi.com
```

If you set "LFCR" for the setting value, it is displayed in a new line in a preview window. For details about the email template definition file, see *4.5.3 Format of the email template definition file*.

For details about elements to be registered from the email body to Items in JP1/Service Support, see the description about the Creating Items by email in the *JP1/Service Support Configuration and Administration Guide*.

4.5.2 Registering the email template definition file

Register the created email template definition file in JP1/OA.

1. Place the email template definition file in JP1/OA.

Place the created email template definition file in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf\template\mail`

For cluster systems:

shared-folder-name`\Analytics\conf\template\mail`

2. Apply the contents of the email template definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the email template definition file to JP1/OA.

Even when you restart the JP1/OA service, all the definition files in the storage folder of the email template definition file are read.

3. Confirm that the contents of the email template definition file were applied.

Select a resource from the **E2E View** window and display the **Execute Action** window, and then confirm that the contents of the email template definition file and the inherited information of the resource are correctly

displayed in a preview window.

Click the **Launch Mailer** button in the action execution window and make sure that the email editor is correctly displayed.

4.5.3 Format of the email template definition file

The email template definition file is a definition file for configuring a template for creating email, to be performed when actions are executed.

Format

Specification key name=setting-value

File

Use any file.

When you save a file, use UTF-8 for the character code of the file.

A maximum of 1000 files can be set in JP1/OA. Files are read in alphabetical order of the file names. If the number of files exceeds 1000, the files after file number 1000 are not read.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf\template\mail`

For cluster systems:

shared-folder-name`\Analytics\conf\template\mail`

Timing of definition application

The definition takes effect when JP1/OA starts or the `reloadproperty` command is executed.

Details of description

Specify a specification key name and its setting value by entering a pair in each line. When you create the email template definition file, note the following points:

- Lines beginning with hash marks (#) are treated as comment lines.
- Blank lines are ignored.
- The setting values are case-sensitive.
- If the setting value is invalid, the default value is set.
- If you specify the same specification key several times in the file, the last specified key is used.
- To specify a tab, specify "\t".
- To display a backslash (\), specify "\\".
- To display a percentage sign (%) in [SE.mail.template.title.string] or [SE.mail.template.body.string], specify "%%".
- When you specify multiple "SE.template.filter.xxxxxxx.string" filter conditions, if all the conditions are met, the

contents of the settings are displayed.

- If you set "LFCR" for the setting value, it is displayed in a new line in a preview window.

Setting elements

Table 4-4 Setting elements of the email template definition file

Key name	Settings	Settable value	Default value
SE.template.name.string	Specifies the action name	Characters within 127 bytes, excluding control characters	Null
SE.template.description.string	Specifies the description about the action	Characters within 255 bytes, excluding control characters	Null
SE.mail.template.title.string	Specifies the subject of the email template	Characters within 255 bytes, excluding control characters	Null
SE.mail.template.body.string	Specifies the body of the email template	Characters within 4096 bytes, excluding control characters	Null
SE.mail.template.address.string	Specifies the address of the email template	Characters within 255 bytes, excluding control characters	Null
SE.template.filter.collectorName.string	Specifies the condition for collector names to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 255 bytes, excluding control characters	Null
SE.template.filter.resourceName.string	Specifies the condition for base resource names to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 255 bytes, excluding control characters	Null
SE.template.filter.resourceType.string	Specifies the condition for base resource types to be displayed in	Characters within 32 bytes, excluding control	Null

Key name	Settings	Settable value	Default value
	the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	characters	
SE.template.filter.vmHostname.string	Specifies the condition for virtual machine names to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 64 bytes, excluding control characters	Null
SE.template.filter.ipaddress.string	Specifies the condition for IP addresses to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 255 bytes, excluding control characters	Null
SE.template.filter.upperResourceName.string	Specifies the condition for base higher resource names to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 512 bytes, excluding control characters	Null
SE.template.filter.upperResourceType.string	Specifies the condition for base higher resource types to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 32 bytes, excluding control characters	Null

Key name	Settings	Settable value	Default value
SE.template.filter.groups.string	Specifies the condition for group name to be displayed in the list of actions at the resource selection. The contents of the settings are displayed only when the action execution window is invoked from resources that satisfy the condition.	Characters within 256 bytes, excluding control characters	Null

You can use the selected resource information as fill character variables for the values of [SE.mail.template.title.string] or [SE.mail.template.body.string].
The following table shows the names of fill character variables.

Table 4-5 List of fill character variables

Variable name	Description	Remarks
%ANALYTICS_RESOURCENAME%	Name of the selected resource	--
%ANALYTICS_UPPERRESOURCENAME%	Name of the higher resource of the selected resource	--
%ANALYTICS_IPADDRESS%	IP address	--
%ANALYTICS_COLLECTORNAME%	Collector server name	--
%ANALYTICS_VIRTUALMACHINENAME%	Virtual machine name	Displayed only for VM resources.
%ANALYTICS_RESOURCETYPE%	Resource type	--
%ANALYTICS_UPPERRESOURCETYPE%	Higher resource type	--
%ANALYTICS_GROUPS%	Group name	--

(Legend) --: Not applicable

If the selected resource has no value to be displayed, a null character is displayed.
To display virtual machines and IP addresses, VMware Tools must be installed on the virtual machine.

Notes

- There is a maximum to the number of characters of the email template definition file that can be displayed in the email editor.

  If the maximum number of specifiable characters is exceeded in an email template's address, subject, and body, clicking the **Launch Mailer** button in the **Execute Action** dialog box might not start the email editor normally.

  If the email editor does not start normally, manually start the email editor, and then copy the contents of the preview to use them.

  The maximum number of specifiable characters differs depending on the web browser used. As a guideline, the

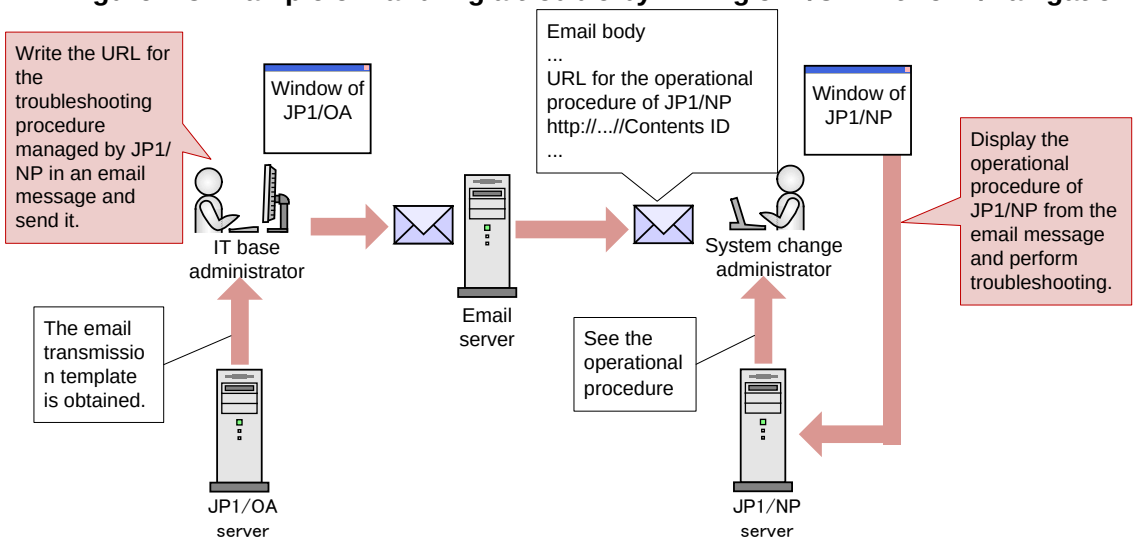
maximum number of characters for web browsers is 2059 characters for Firefox, and 200 characters for Internet Explorer 11.

4.6 Linkage with JP1/Navigation Platform

Linkage with JP1/Navigation Platform allows you to analyze the cause of error occurrence and provide potential means to handle the problem by JP1/OA.

The following figure shows an example of handling a problem by linking JP1/OA with JP1/Navigation Platform.

Figure 4-3 Example of handling a trouble by linking JP1/OA with JP1/Navigation Platform



This section describes the procedure for linking JP1/OA with JP1/Navigation Platform.

4.6.1 Create an email template definition file (for linkage with JP1/NP)

Create an email template definition file used for providing the business contents of JP1/Navigation Platform.

1. Create an email template definition file.

Create an email template definition file. You can specify any value for the file name and extension.

The email template definition file must be saved in UTF-8 file format.

Definition example when setting the selected resource name for the subject

SE.template.name.string=001_JP1/NP email creation for troubleshooting request
SE.template.description.string=Create an email to tell the person responsible the URL for JP1/NP operational procedures.
SE.mail.template.title.string=Subject: Request to change the HDD capacity (%ANALYTICS_RESOURCENAME%)
SE.mail.template.body.string=Body: LFCRvCenter name: %ANALYTICS_COLLECTORNAME%LFCRDetails of request: Increase the HDD capacity of the corresponding host. Details of work: LFCR http://***host-name***:***port-number***/ucnpBase/..../default?open...& contentId=***business-contents-ID***
SE.mail.template.address.string=xxxxxxx@hitachi.com

If you set "LFCR" for the setting value, it is displayed in a new line in a preview window. For details about the email template definition file, see *4.5.3 Format of the email template definition file*.

For details about the URL specification for displaying the business contents of JP1/Navigation Platform, see the description about the Parameters that can be specified for the basic URL in the *Hitachi Navigation Platform Content Editing Guide*.

4.6.2 Registering the email template definition file

Register the created email template definition file in JP1/OA.

1. Place the email template definition file in JP1/OA.

Place the created email template definition file in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf\template\mail`

For cluster systems:

shared-folder-name`\Analytics\conf\template\mail`

2. Apply the contents of the email template definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the email template definition file to JP1/OA.

Even when you restart the JP1/OA service, all the definition files in the storage folder of the email template definition file are read.

3. Confirm that the contents of the email template definition file were applied.

Select a resource from the **E2E View** window and display the **Execute Action** window, and then confirm that the contents of the email template definition file and the inherited information of the resource are correctly displayed in a preview window.

Click the **Launch Mailer** button in the action execution window and make sure that the email editor is correctly displayed.

4.7 Command linkage with other products

You can use the **Execute Action** window to execute the commands of other products, user programs, and other resources on the server where JP1/OA is installed.

4.7.1 Creating a command template definition file

Create a command template definition file. You can specify any file name and file extension you like.

Command template definition files must be saved in UTF-8 format.

Definition example where the selected resource names are specified for command arguments

```
SE.template.name.string=001_task-execution
SE.template.description.string=Runs the scheduled tasks.
SE.cmd.template.cmdName.string=schtasks
SE.cmd.template.cmdArgs.string=/run /tn /*TaskName*/ /s %ANALYTICS_RESOURCENAME% /*User*/
```

4.7.2 Registering the command template definition file

Register the created command template definition file in JP1/OA.

1. Deploy the command template definition file to JP1/OA.

Save the created command template definition file in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf\template\command`

For cluster systems:

shared-folder-name`\Analytics\conf\template\command`

2. Apply the contents of the command template definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the command template definition file to JP1/OA.

Even if the JP1/OA service is restarted, all of the definition files in the folder containing the command template definition file will be loaded.

4.7.3 Format of command definition files

Command definition files are used to set up templates for the commands to be executed in the **Execute Action** window.

Format

specified-key-name=specified-value

File

Use any file.

Save the file with UTF-8 encoding.

The maximum number of files that can be set in JP1/OA (including the number of email template definition files) is 1,000. Files are loaded in alphabetical order by file name, and any files after the 1,000th file will not be loaded.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf\template\command

For cluster systems:

shared-folder-name\Analytics\conf\template\command

Definition application timing

When JP1/OA is started or the `reloadproperty` command is executed

Content to be specified

Specify each key name and value on a single line. Note the following when specifying settings in a command template definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- Definitions are case-sensitive.
- If an invalid value is specified, the default value is used.
- If the same key is specified more than once in the same file, the last specification is valid.
- To specify a tab, specify "\t".
- To display a backslash (\), specify "\\".
- To display a percentage sign (%) in [SE.cmd.template.cmdArgs.string], specify "%%".
- If the filter condition SE.template.filter.*xxxxxxx*.string is specified more than once, settings will be displayed when all of the conditions are met.

Settings

Table 4-6 Settings in the command template definition file

Key name	Setting description	Specifiable values	Default value	Optional or required
SE.template.name.string	Specify the action name.	Values of no more than 127	#1	Required

Key name	Setting description	Specifiable values	Default value	Optional or required
		bytes and that do not include control characters		
SE.template.description.string	Specify a description of the action.	Values of no more than 255 bytes and that do not include control characters	Null character	Optional
SE.cmd.template.cmdName.string	Specify the name of the command to be executed by specifying the absolute path to the command. Execution of a command specified by its relative path might fail.	Values of no more than 255 bytes and that do not include control characters	#1	Required
SE.cmd.template.cmdArgs.string	Specify arguments for the command to be executed.	Values of no more than 4,096 bytes and that do not include control characters	Null character	Optional
SE.cmd.template.timeOut.num	Specify the timeout period for the command to be executed (in milliseconds).	1 to 2147483647	30000	Optional
SE.template.filter.collectorName.string	Specify conditions for the collector server names that are to be displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	Values of no more than 255 bytes and that do not include control characters	Null character	Optional
SE.template.filter.resourceName.string	Specify conditions for the names of the resources that are starting points	Values of no more than 255	Null character	Optional

Key name	Setting description	Specifiable values	Default value	Optional or required
	and that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	bytes and that do not include control characters		
SE.template.filter.resourceType.string	Specify conditions for the types of resource that are starting points and that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	Values of no more than 32 bytes and that do not include control characters	Null character	Optional
SE.template.filter.vmHostname.string	Specify conditions for the virtual machine names that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	Values of no more than 64 bytes and that do not include control characters	Null character	Optional
SE.template.filter.ipaddress.string	Specify conditions for the IP addresses that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	Values of no more than 255 bytes and that do not include control characters	Null character	Optional
SE.template.filter.upperResourceName.string	Specify conditions for the names of higher-level resources of a starting point that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is	Values of no more than 512 bytes and that do not include control characters	Null character	Optional

Key name	Setting description	Specifiable values	Default value	Optional or required
	called from a resource that matches the specified conditions.			
SE.template.filter.upperResourceType.string	Specify conditions for the types of higher-level resources of a starting point that are displayed in the action list during resource selection. Settings are displayed only when the **Execute Action** window is called from a resource that matches the specified conditions.	Values of no more than 32 bytes and that do not include control characters	Null character	Optional
SE.template.filter.groups.string	Specify conditions for group names to be displayed in the list of actions when resources are selected. Settings are displayed only when the **Execute Action** window is invoked from a resource that matches the specified conditions.	Values of no more than 255 bytes and that do not include control characters	Null character	Optional

#1: This setting has no default value, because specification of this setting is required.

You can use the selected resource information as fill character variables for the values of [SE.cmd.template.cmdArgs.string].
The table below lists the variables that can be used.

Table 4-7 Variables

Variable name	Description	Remarks
%ANALYTICS_RESOURCENAME%	Name of the selected resource	--
%ANALYTICS_UPPERRESOURCENAME%	Name of the higher-level resource of the selected resource	--
%ANALYTICS_IPADDRESS%	IP address	--
%ANALYTICS_COLLECTORNAME%	Name of the collector server	--
%ANALYTICS_VIRTUALMACHINENAME%	Name of the virtual machine	Displayed only when the resource is a virtual machine.
%ANALYTICS_RESOURCETYPE%	Resource type	--
%ANALYTICS_UPPERRESOURCETYPE%	Type of the higher-level resource	--

Variable name	Description	Remarks
%ANALYTICS_GROUPS%	Group name	--

(Legend) --: Not applicable

If no value is set for the selected resource, a null character is displayed.

To display information about virtual machines and IP addresses, VMware Tools must be installed on virtual machine.

5.Direct Access URL

In JP1/OA, you can directly display the desired window after login by specifying the URL of the operation window. This functionality is called the *direct access URL function*.

Only the following windows can be displayed by specifying direct access URLs:

- Dashboard window
- Event window
- Search Resources window
- JP1/OA management window

5.1 Specification format and elements of a direct access URL

A direct access URL consists of the basic URL and parameters for specifying the window to be displayed and information to be displayed in the window. The basic URL and each parameter are delimited by question marks (?).

The string to be specified at the beginning of a direct access URL differs depending on the communication method used between the web browser and the JP1/OA server. The description below is for HTTP connections. Replace "http" with "https" as necessary.

If the specification of the basic URL is invalid, the **Login** window does not appear and an error message for the web client or web server is displayed.

The following rules apply to parameters:
- Use an ampersand (&) to separate parameter keys.
- When you specify multibyte characters for the specification value of a parameter, perform URL encoding for the characters by using UTF-8.
- If a key specification is duplicated, the last specified key is used.

The following is the specification format of a direct access URL:

http://***host-name***:***port-number***/Analytics/main.htm?module=***ID-of-window-to-be-displayed***&param[***key-name***]=***key-value***

Basic URL | module parameter | param parameter

The following table shows the specification elements of a direct access URL.

Table 5-1 Specification elements of a direct access URL

No.	Configuration element	Specification item	Description
1	Basic URL	**Host name**	Specify the host name or IP address of the JP1/OA server.
2		**Port number**	Specify the port number of the web server of JP1/OA. The default value is 22015.
3	module parameter	**ID of the window to be displayed**	Specify the window to be displayed. You can specify the following values: **- dashboard** Displays the Dashboard window. **- analytics** Displays the Search Resources window. **- event** Displays the Event window. **- administration** Displays the JP1/OA management window. If you do not specify the module parameter and a value, the Dashboard window appears.
4	param parameter	param[searchType]=**search-resource-type**	Specify the type of the resource to search for in the searchType parameter. You can specify the following values: **- groups** Searches for "Consumers". **- servers** Searches for "Servers". **- switches** Searches for "Switches". **- storages** Searches for "Storage systems". **- volumes** Searches for "Volumes". If you specify a null character or do not specify any value, groups is set.
5		param[searchKey]=**search-resource-name**	Specify the characters to search for in the searchKey parameter. Note that ampersands (&) and equal signs (=)

No.	Configuration element	Specification item	Description
			are reserved characeres and cannot be specified in search resource names. In addition, if you specify a null character, all of the resource names are acquired.

Example of a URL to display the Dashboard window

http://***host-name***:22015/Analytics/main.htm?module=dashboard

Example of a URL to specify a server name for the search keyword and display the Search Resources window

http://***host-name***:22015/Analytics/main.htm?module=analytics&param[searchType]=servers& param[searchKey]=***search-server-name***

Note: Write the URL on a single line.

6. Monitoring Applications

You can use JP1/OA to manage IT infrastructure systems that include applications. The method for configuring monitoring and the customization method differ depending on the type of application being monitored: for example, whether the application is managed by a JP1 product or whether the application is a third-party product's application. The following diagram shows the areas whose content can be customized when an application is monitored. The numbers in the diagram corresponds to the numbers in the table after the diagram.

Figure 6-1 Areas that can be customized when an application is monitored

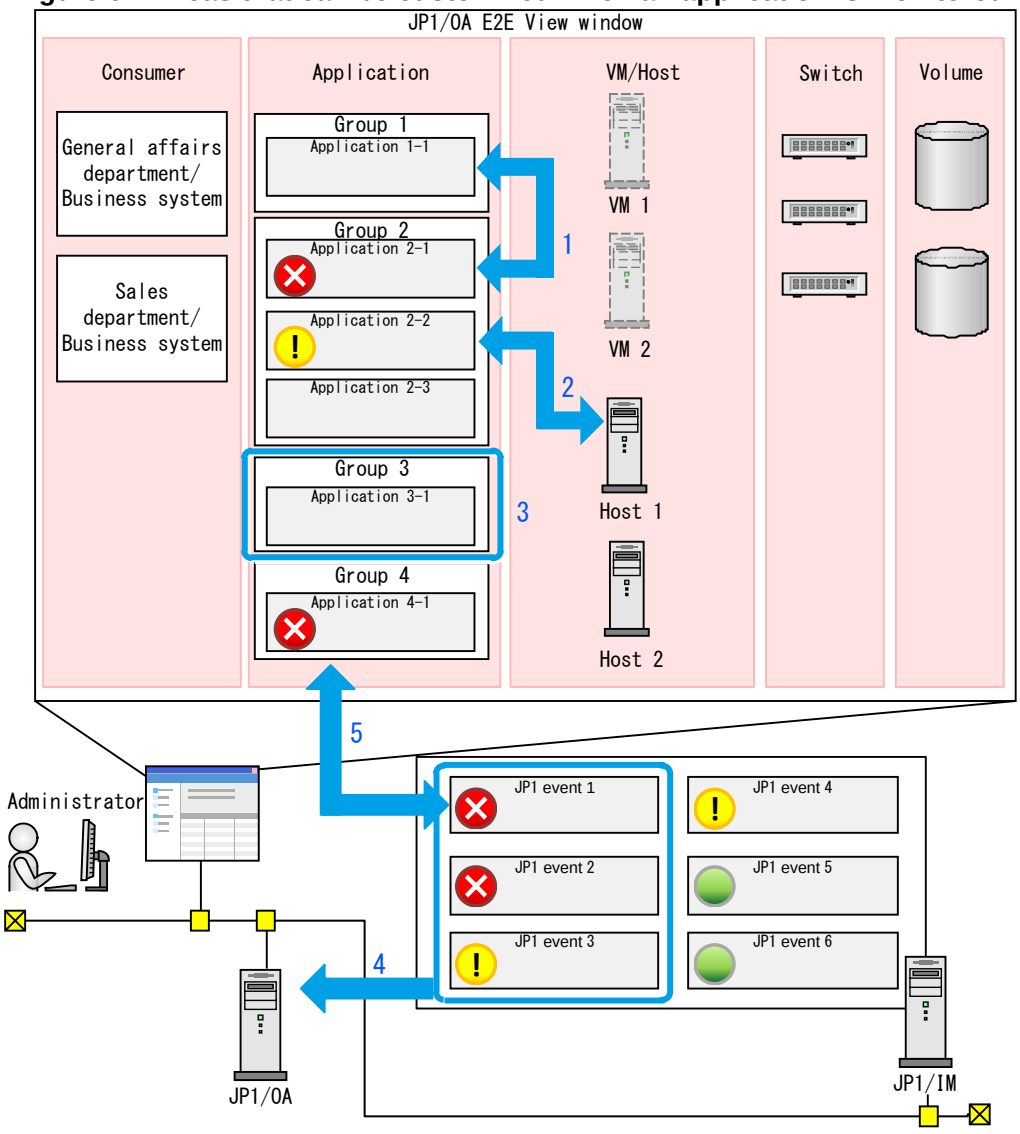


Table 6-1 Overview of customization related to application monitoring

No.	Summary	Description	Refer to:	
			When monitoring JP1 products	When monitoring any other application
1	Mapping between applications	You can add or change the associations, displayed in the **E2E View** window, between applications.	6.2.1	6.4.1
2	Mapping between applications and hosts	You can add or change the associations, displayed in the **E2E View** window, between applications and hosts.	6.2.2	6.4.2
3	Defining a grouping of applications	You can add or change the method for grouping applications in the **E2E View** window and **Dashboard** window.	6.2.3	6.4.3
4	Defining JP1 events to be obtained from JP1/IM	If JP1/IM is registered as a collector, you can define conditions for obtaining JP1 events.	6.2.4	
5	Defining mapping target for JP1 events	You can change the application that becomes the mapping target of an obtained JP event.	6.2.5	6.4.4

6.1 Settings for monitoring applications by linking with JP1 products

To manage IT infrastructure systems (including applications) by linking with JP1 products, specify the settings required for linkage and then register the JP1 products as collectors in the **Management Tool Registration** window. For details on how to specify the settings required for linkage, see *4.2 Linkage with a Windows version of a JP1 product* or *4.3 Linkage with the UNIX version of JP1 products*. For details on how to register tools to be managed, see the *JP1 Version 11 Integrated Management Getting Started (IT Operations Analytics)*.

6.2 Customizing application monitoring by linking with JP1 products

By customizing the associations between applications, users can more easily understand and analyze the structure of the IT infrastructure system.

6.2.1 Mapping between applications

When related applications are associated with each other, the **E2E View** window displays the associations between the applications. If JP1 products are to be monitored and the JP1 products meet certain conditions when the JP1 products are registered, the applications will automatically be associated with each other.

The following applications will be automatically associated with each other:
- JP1/AJS3 - Manager and JP1/AJS3 - Agent

The following applications will be automatically associated with each other if they exist on the same host:
- JP1/Base (OS) managed by JP1/IM - Manager and JP1/PFM - Agent (OS, DBMS, etc.)
- JP1/Base (OS) managed by JP1/IM - Manager and JP1/AJS3 - Manager
- JP1/Base (OS) managed by JP1/IM - Manager and JP1/AJS3 - Agent
- JP1/PFM - Agent (OS, DBMS, etc.) and JP1/AJS3 - Manager
- JP1/PFM - Agent (OS, DBMS, etc.) and JP1/AJS3 - Agent

For applications that cannot be automatically associated, use definition files to associate them with each other.

(1) Creating application mapping definition files

Use the following procedure to create a definition file (`appMapping.conf`) that associates applications with each other.

1. Create the application mapping definition file in CSV format.
For details about the definition file, see *(3) Format of application mapping definition files*.

2. Save the definition file.
Specify `appMapping.conf` as the file name and extension.
Save the file with UTF-8 encoding.

(2) Registering application mapping definition files

Register the created application mapping definition files in JP1/OA.

1. Place application mapping definition files in JP1/OA.
Place the created application definition files in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf

For cluster systems:

shared-folder-name*Analytics*\conf

2. Apply the application mapping definition file to JP1/OA.

After this definition file is saved, it will be read automatically the next time when **E2E View** window be displayed.

3. Confirm that the content of the application mapping definition files has been applied.

Display the **E2E View** window, and confirm that the icons of the applications associated with the application used as the base point of mapping are highlighted.

(3) Format of application mapping definition files

This file defines the mapping between applications.

Format

#ResourceID,Parent Resource ID,Parent Resource Type,Related Resource ID,Related Parent Resource ID,Related Parent Resource Type,Type

host-name, *host-name-of-collector*, *product-name-of-collector*, *host-name-of-mapping-target*, *host-name of-collector-of-mapping-target*, *product-name-of-collector-of-mapping-target*, *type*

:

File

appMapping.conf

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf

For cluster systems:

shared-folder-name\Analytics\conf

Definition application timing

The next time when **E2E View** window be displayed after this definition file is saved.

Content to be specified

In CSV format, specify the information about the applications for which you want to add or remove associations.

Note the following when specifying settings in a definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- The entries are case sensitive.

Settings

Items to define are described in the table below. If the applications for which mapping is to be defined have already been registered in JP1/OA, you can check the details of values to be specified for each column in the JP1/OA window. If the applications are not yet registered, make sure that the settings specified when registering the management software are the same as the content of the definition files.

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
ResourceID	Host name or service ID for the application for which you want to specify an association	- Host name for JP1/Base, JP1/AJS3 - Manager, or JP1/AJS3 - Agent - Service ID for JP1/PFM - Agent	From the **E2E View** window, select the application, and then click **Show Detail** to display the application details window. In that window, click the **Basic Information** tab.#
Parent Resource ID	IP address or host name of the collector for the application for which you want to specify an association	IP address or host name for JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	The **IP Address/Host Name** column in the **Application** tab in the **Management Tool Registration** window
Parent Resource Type	Product name of the collector for the application for which you want to specify an association	Product name (`JP1/IM - Manager`, `JP1/AJS3 - Manager`, or `JP1/PFM - Manager`)	The **Product Name** column in the **Application** tab in the **Management Tool Registration** window
Related Resource ID	Host name or service ID of the application for which you want to add or remove an association. This application was specified in ResourceID.	- Host name for JP1/Base, JP1/AJS3 - Manager, or JP1/AJS3 - Agent - Service ID for JP1/PFM - Agent	From the **E2E View** window, select the application, and then click **Show Detail** to display the application details window. In that window, click the **Basic Information** tab.#

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
Related Parent Resource ID	Host name or service ID of the collector for the application for which you want to add or remove an association. This application was specified in ResourceID.	IP address or host name of JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	The **IP Address/Host Name** column in the **Application** tab in the **Management Tool Registration** window
Related Parent Resource Type	Product name of the collector for the application for which you want to add or remove an association. This application was specified in ResourceID.	Product name (`JP1/IM - Manager`, `JP1/AJS3 - Manager`, or `JP1/PFM - Manager`)	The **Product Name** column in the **Application** tab in the **Management Tool Registration** window
Type	Type of operation (add or remove)	- Specify `Add` to add an association. - Specify `Remove` to remove an existing association.	--

(Legend) --: Not applicable

#: The host names for JP1/Base and JP1/AJS3 are displayed in the **Name** column of the detailed window. The JP1/PFM service ID is displayed in the **Service ID** column in the detailed window.

Definition example

The following example shows what to input to define the following content:

Definition example 1:

Add an association between JP1/AJS3 - Agent (Host name: `AgtHost01`) and JP1/PFM - Agent (Service ID: `7A1Remote2[JH22957vm4R8002@PFM-HOST01]`).

The collector for JP1/AJS3 - Agent is JP1/AJS3 - Manager (IP address: `192.168.10.10`).

The collector for JP1/PFM - Agent is JP1/PFM - Manager (IP address: `192.168.20.20`).

Definition example 2:

Add an association between JP1/PFM - Agent (Service ID: `TA1PFMA4P-HOST01`) and JP1/AJS3 - Manager (IP address: `192.168.10.10`).

The collector for JP1/PFM - Agent is JP1/PFM - Manager (IP address: `192.168.20.20`).

The collector for JP1/AJS3 - Manager is JP1/AJS3 - Manager itself.

Input example:

```
#ResourceID,Parent Resource ID,Parent Resource Type,Related Resource ID,Related Parent Resource ID,Related Parent Resource Type,Type
AgtHost01,192.168.10.10,JP1/AJS3 - Manager,7A1Remote2[JH22957vm4R8002@PFM-HOST01],192.168.20.20,JP1/PFM - Manager,Add
TA1PFMA4P-HOST01,192.168.20.20,JP1/PFM - Manager,MgrHost01,192.168.10.10,JP1/AJS3 - Manager,Add
```

6.2.2 Mapping between applications and hosts

When the JP1 products are registered from the **Management Tool Registration** window, if the host names obtained from the applications associated with the JP1 products match the names of hosts managed by JP1/OA, the applications and hosts will automatically be associated. If the applications and hosts cannot be automatically associated or if there are unnecessary associations, use the application-host mapping definition file for applications and hosts to add or remove the associations between the applications and hosts.

You can use the application-host mapping definition file for the following purposes:

- To add or remove an association between an application and a host
  For example, if multiple hosts with the same name exist and unnecessary associations are automatically made, you can use the definition file to remove the unnecessary associations.
  To add the associations, in the definition file specify `Add` for Type. To remove the associations, in the definition file specify `Remove` for Type.

- To specify that the host names obtained from applications are to be regarded as the host names managed by JP1/OA
  For example, if the host name obtained from an application associated with a JP1 product is the host name or alias name of a logical host and the name differs from the host name managed by JP1/OA, the application and the host cannot be associated automatically. In such a case, use the definition file to specify that the host name or alias name of the logical host obtained from the application is to be regarded as the host name managed by JP1/OA. This enables you to associate the application and the host.
  To specify that the obtained host name is to be regarded as the host name managed by JP1/OA, specify `RegardAs` in Type.

Note that applications will belong to the same consumers as those to which automatically-associated hosts belong. Therefore, if you change the associations between the applications and hosts, the consumers to which the applications belong might change depending on the associated hosts.

(1) Creating an application-host mapping definition file

Use the following procedure to create a definition file (`appHostMapping.conf`) that adds or removes

associations between applications and hosts.

1. Create an application-host mapping definition file in CSV format.

For details about the definition file, see *(3) Format of the application-host mapping definition file.*

2. Save the definition file.

Specify `appHostMapping.conf` as the file name and extension.

Save the file with UTF-8 encoding.

(2) Registering the application-host mapping definition file

Register the created application-host mapping definition file in JP1/OA.

1. Place the application-host mapping definition file in JP1/OA.

Place the created application-host mapping definition file in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

2. Apply the application-host mapping definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the application-host mapping definition file to JP1/OA.

Alternatively, you can restart the JP1/OA service to load the contents of the application-host mapping definition file.

3. Confirm that the contents of the application-host mapping definition file have been applied.

Display the **E2E View** window, and confirm that the icons of the hosts associated with the application used as the base point are highlighted, or that the icons of the hosts for which you want to remove the association with the application used as the base point are not highlighted.

(3) Format of the application-host mapping definition file

This file defines the mapping between applications and hosts.

Format

#App Host Name/App Resource ID,Parent Resource ID,Parent Resource Type, Regarded Host Name/Host Resource ID,Type

host-name, *host-name-of-collector*, *product-name-of-collector*, *host-name-managed-by-JP1/OA*, *type*

:

File

`appHostMapping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

Definition application timing

When JP1/OA is started or the `reloadproperty` command is executed.

Content to be specified

In CSV format, specify the information about the applications and hosts for which you want to add or remove associations.

Note the following when specifying settings in a definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- The entries are case sensitive.

Settings

Items to define are described in the table below. If the applications for which mapping is to be defined have already been registered in JP1/OA, you can also check the details of the settings to be specified for each column in the JP1/OA window. If the applications are not yet registered, make sure that the settings specified when registering the management software are the same as the contents of the definition file.

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
App Host Name/ App Resource ID	Host name or service ID for the application for which you want to specify an association	If you want to add or remove an association between an application and a host (by specifying `Add` or `Remove` in Type), specify the following: - Host name for JP1/Base, JP1/AJS3 - Manager, or JP1/AJS3 - Agent - Service ID for JP1/PFM - Agent	From the **E2E View** window, select the application, and then click **Show Detail** to display the application details window. In that window, click the **Basic Information** tab.#
		If you want to regard the host name or alias name of the logical host obtained from the applications as the host name managed by JP1/OA (by specifying `RegardAs` in Type), specify the host name (that is, the host name or alias name of logical host obtained from the applications).	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Parent Resource ID	IP address or host name of the collector for the application for which you want to specify an association	IP address or host name for JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	The **IP Address/Host Name** column in the **Application** tab in the **Management Tool Registration** window.
Parent Resource Type	Product name of the collector for the application for which you want to specify an association	Product name (`JP1/IM - Manager`, `JP1/AJS3 - Manager`, or `JP1/PFM - Manager`)	The **Product Name** column in the **Application** tab in the **Management Tool Registration** window.
Regarded Host Name/Host Resource ID	Name of the host to be associated you want to associate with the host name obtained from the application, or ID of the host to be associated with	If you want to add or remove an association between an application and a host (by specifying `Add` or `Remove` in Type), specify the ID of a host managed by JP1/OA.	The **ID** column of the output results of the `listresources` command.

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
	or disassociated from the application	If you want the host name or alias name of the logical host obtained from the application to be regarded as the host name managed by JP1/OA (by specifying `RegardAs` in Type), specify the host name managed by JP1/OA.	The **Host Name** column in the **Basic Information** tab in the virtual machine details or host details window. To display the virtual machine details or host details window, from the **E2E View** window, select the virtual machine or host, and then click **Show Detail**.
Type	Type	- Specify `Add` to add an association between applications and hosts. - Specify `Remove` to remove the association between applications and hosts. - Specify `RegardAs` if you want the host name or alias name of the logical host obtained from the application to be regarded as the host name managed by JP1/OA.	--

(Legend) --: Not applicable

#: The host names for JP1/Base and JP1/AJS3 are displayed in the **Name** column of the detailed window. The JP1/PFM service ID is displayed in the **Service ID** column of the details window.

Definition example

The following shows an input example for defining the following associations:

Definition example 1:

The host name (`IMA001`) of the application obtained from the collector is to be regarded as the host name (`TA2IMA4P-HOST02`) of the host managed by JP1/OA, for the association between the application and the host.
The collector for the application is JP1/IM - Manager (IP address: `192.168.20.30`).

Definition example 2:

Remove the association between JP1/AJS3 - Agent (Host name: `AgtHost01`) and the host (ID: `vm6`) that is managed by JP1/OA.
The collector for JP1/AJS3 - Agent is JP1/AJS3 - Manager (IP address: `192.168.10.10`).

Input example:

```
#App Host Name/App Resource ID,Parent Resource ID,Parent Resource Type, Regarded Host Name/Host Resource ID,Type
IMA001,192.168.20.30,JP1/IM - Manager,TA2IMA4P-HOST02,RegardAs
AgtHost01,192.168.10.10,JP1/AJS3 - Manager,vm6,Remove
```

6.2.3 Defining a grouping of applications

In JP1/OA, the **E2E View** window and the **Dashboard** window display applications associated with linked JP1 products in groups, according to the grouping definitions.

You can customize a definition file for grouping applications to move a specific type of application to a different group, or to create a new group. For the types of applications, see *Table 6-2 Application types that can be specified.*
If you edited a definition file for grouping applications, and then applied the definitions in the file to JP1/OA, applications are grouped based on the definitions in the definition file for grouping applications. Types of applications that are not included in the definitions in the customized definition file are grouped and displayed based on the default grouping definitions of JP1/OA.

(1) Editing the definition file for grouping applications

In the following definition file for grouping applications, edit the new grouping information to specify new grouping information.
Save the file with UTF-8 encoding.

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf\template\appGrouping.conf

For cluster systems:

shared-folder-name\Analytics\conf\appGrouping.conf

For details about the definition file for grouping applications, see *(3) Format of the definition file for grouping applications*.

(2) Applying the definition file for grouping applications

Apply the definition file for grouping applications to JP1/OA.

1. Apply the definition file for grouping applications.

After this definition file is saved, it will be read automatically the next time when **E2E View** window or **Dashboard** window be displayed.

2. Confirm that the contents of the definition file for grouping applications have been applied.

Display the **E2E View** window, and confirm that the applications displayed in the application area are grouped

according to the edited definitions.

Display the **Dashboard** window, and confirm that the groups displayed in the application summary in the (Main Report) System Status Summary for Application Administrators report match the top three groups defined in the edited definition file.

(3) Format of the definition file for grouping applications

Application grouping definition files are used to define a grouping of applications.

Format

group-name-1
{
application-type-1
application-type-2
:
:
}
group-name-2
{
application-type-3
application-type-4
:
:
}
:
:

File

`appGrouping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

When the definitions are applied

The next time when **E2E View** window or **Dashboard** window be displayed after this definition file is saved.

Description

The definition file specifies the group name and the types of applications that will belong to the group for each group.

The **E2E View** window displays applications based on the group definitions specified in the definition file for grouping applications. If an application type is not defined (the types are listed in *Table 6-2 Application types that can be specified*), the specified application type follows the default grouping definition, and are complemented and displayed.

The top three groups defined in the definition file are displayed in the application summary in the (Main Report) System Status Summary for Application Administrators report in the **Dashboard** window. If the number of groups defined in the file is less than three, groups defined in the default grouping definitions will be added so that three groups are displayed.

Note the following when specifying the definition file:

- Lines beginning with a hash mark (#) are treated as comment lines.
- Blank lines are ignored.
- Alphabetic characters are case sensitive.

Setting items

1. Group name

Specify the name for identifying the group.

Specify the group name by using 128 or fewer characters.

2. Application type

Specify the type of applications that will belong to the group.

The following table lists the values for application types that can be specified.

Table 6-2 Application types that can be specified

No.	Specifiable setting values	Application types
1	AJS	JP1/AJS3 (Manager) or JP1/AJS3 (Agent)
2	PFM_SERVICERESPONSE	JP1/PFM (ServiceResponse)
3	PFM_AJS3	JP1/PFM (JP1/AJS3)
4	PFM_DOMINO	JP1/PFM (Domino)
5	PFM_EXCHANGE	JP1/PFM (Exchange)
6	PFM_SAPSYSTEM	JP1/PFM (SAP System)
7	PFM_IBMWEBSPHEREMQ	JP1/PFM (IBMWebSphereMQ)
8	PFM_OPENTP1	JP1/PFM (OpenTP1)
9	PFM_COSMINEXUS	JP1/PFM (Cosminexus)
10	PFM_IIS	JP1/PFM (IIS)
11	PFM_WEBLOGICSERVER	JP1/PFM (WebLogic Server)

No.	Specifiable setting values	Application types
12	PFM_WEBSPHEREAPPLICATIONSERVER	JP1/PFM (WebSphere Application Server)
13	PFM_DB2	JP1/PFM (DB2)
14	PFM_HIRDB	JP1/PFM (HiRDB)
15	PFM_SQL	JP1/PFM (SQL)
16	PFM_RMSQLSERVER	JP1/PFM (RM SQLServer)
17	PFM_ORACLE	JP1/PFM (Oracle)
18	PFM_RMORACLE	JP1/PFM (RM Oracle)
19	PFM_RMPLATFORM	JP1/PFM (RM Platform)
20	PFM_UNIX	JP1/PFM (UNIX)
21	PFM_WINDOWS	JP1/PFM (Windows)
22	IM_OS	JP1/IM

Definition example (system's default grouping definitions)

The following example shows the system's default grouping definitions.

```
Job
{
AJS
}
Service Response
{
PFM_SERVICERESPONSE
}
Enterprise
{
PFM_AJS3
PFM_DOMINO
PFM_EXCHANGE
PFM_SAPSYSTEM
}
Transaction Processing
{
PFM_IBMWEBSPHEREMQ
PFM_OPENTP1
}
Application Server
{
PFM_COSMINEXUS
PFM_IIS
PFM_WEBLOGICSERVER
PFM_WEBSPHEREAPPLICATIONSERVER
}
Database
{
PFM_DB2
PFM_HIRDB
PFM_SQL
PFM_RMSQLSERVER
PFM_ORACLE
PFM_RMORACLE
}
Platform
{
PFM_RMPLATFORM
PFM_UNIX
PFM_WINDOWS
}
Other Applications
{
IM_OS
}
```

6.2.4 Defining JP1 events to be obtained from JP1/IM

If JP1/IM is registered as a collector in JP1/OA, the default setting is that JP1/OA obtains all the JP1 events of JP1/IM. If you want to obtain specific JP1 events, you can specify the events to be obtained from JP1/IM in the JP1 event definition file.

(1) Creating a definition file for JP1 events to be obtained from JP1/IM

Use the following procedure to create a definition file (`tgtEvent.conf`) that specifies JP1 events to be obtained from JP1/IM.

1. Create a definition file for JP1 events to be obtained from JP1/IM.

For details about the definition file, see *(3) Format of the definition file for JP1 events to be obtained from JP1/IM*.

2. Save the definition file.

For the file name and the file extension, specify `tgtEvent.conf`.

Save the file with UTF-8 encoding.

(2) Registering the definition file for JP1 events to be obtained from JP1/IM

This section describes how to register the created definition file for JP1 events to be obtained from JP1/IM to JP1/OA.

1. Place the definition file for JP1 events to be obtained from JP1/IM in JP1/OA.

Place the created definition file for JP1 events to be obtained from JP1/IM in the following folders:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

2. Apply the definition file for JP1 events to be obtained from JP1/IM to JP1/OA.

After this definition file is saved, it will be read automatically when any of the following operations is performed:

- The next time that events are collected
- When the **E2E View** window displays application details
- When the **Event Analysis View** window collects event details

(3) Format of the definition file for JP1 events to be obtained from JP1/IM

This section describes the file which defines JP1 events to be obtained from JP1/IM.

Format

event-condition

:

OR

event-condition

:

EXCLUDE

event-condition

:

File

`tgtEvent.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

When the definitions are applied

After this definition file is saved, it will be read automatically when any of the following operations is performed:

- The next time that events are collected
- When the **E2E View** window displays application details
- When the **Event Analysis View** window collects event details

Description

The definition file specifies JP1 events to be obtained from JP1/IM by specifying pass-conditions groups and exclusion-conditions groups.

The maximum size of the file is 256 kilobytes (262,144 bytes).

Note the following when specifying the definition file.

- Lines beginning with hash mark "#" are treated as comment lines.
- Blank lines are ignored.
- The entries are case sensitive.

Setting items

1. Pass-conditions groups and exclusion-conditions groups

JP1 events to be obtained are those that do not match with exclusion conditions groups and that match with one of

pass-conditions groups.

You can specify 0 to 5 pass-conditions groups and 0 to 5 exclusion-conditions groups as the filtering conditions.

You can specify 0 to 50 event conditions for pass-conditions groups or exclusion-conditions groups.

Conditions groups separator	Description
OR	If you specify multiple condition groups, specify `OR` between specified condition groups.
EXCLUDE	- Specify `EXCLUDE` between pass-conditions groups and exclusion-conditions groups. - Event conditions described after `EXCLUDE` are considered as exclusion-conditions groups. - If no event conditions are described after the `EXCLUDE`, only the pass-conditions groups will be enabled.

2. Event condition

Event conditions are specified in the following format (__ indicates a space).

Attribute name__Comparison keyword__Operand[__Operand]...

Note that a line which includes only spaces or tabs is ignored during processing.

Attribute name

Specify the name of the attribute that you want to compare.

Comparison keyword

Specify one of `BEGIN` (begins with), `IN` (matches), `NOTIN` (does not match), `SUBSTR` (includes), `NOTSUBSTR` (do not include), or `REGEX` (regular expression) as the comparison keyword.

Operand

Specify a character string as the value that is to be compared with the attribute value by the comparison keyword.

If you specify multiple operands, separate the operands with one or more consecutive spaces or a tab. The OR condition is applied to the specified operands. Note that if you specify a regular expression as the comparison keyword, you can specify only one operand.

To specify a space, a tab, end-of-line code (CR or LF) or % as part of an operand, specify as shown in the following table.

No.	Value to be set	How to specify
1	Tab (0x09)	`%09`
2	Space (0x20)	`%20`
3	% (0x25)	`%25`

No.	Value to be set	How to specify
4	Linefeed code LF (0x0a)	%0a
5	Carriage return code CR (0x0d)	%0d

During maximum value checking for the definition format, %20 and %25 are each treated as a single character. The character code specified after the % is not case sensitive. The following shows an example of defining ID matches 100 and 200, which selects multiple operands:

B.ID__IN__100__200

__: Space (0x20)

You can specify a maximum of 4,096 bytes of operands per event condition (total length in bytes of all operands that are specified in the event condition block).

The following table lists attribute names, comparison keywords, and operands that can be specified for the event condition.

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	B.ID	- IN (matches) - NOTIN (does not match)	- Multiple event IDs can be specified. A maximum of 100 event IDs can be specified. - Event IDs are not case sensitive. - Permitted range is from 0 to 7FFFFFFF.
2	Event-issuing server name	B.SOURCESERVER	- BEGIN (begins with) - IN (matches) - NOTIN (does not match) - SUBSTR (includes) - NOTSUBSTR (do not include) - REGEX (regular expression)	- Multiple items can be specified. A maximum of 100 items can be specified. However, if a regular expression is used, only one item is allowed.
3	Message	B.MESSAGE		
4	Product name	E.PRODUCT_NAME		
5	Object ID	E.OBJECT_ID		
6	Event sourcehost name	E.JP1_SOURCEHOST		
7	Severity	E.SEVERITY	IN (matches)	- The following are the specifiable values: Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug. - Multiple severity values can be specified. However same severity is not allowed.

Example definition

The following shows an example of a definition that obtains a JP1 event from JP1/IM when the event ID is `101` or `102` and the severity level is Error, and the event-issuing server name is not `host3`.

```
B.ID IN 101 102
OR
E.SEVERITY IN Error
EXCLUDE
B.SOURCESERVER IN host3
```

Notes

- Note on the status of errors and warnings displayed for applications in the **E2E View** window

  The status of errors and warnings before this file is applied are not reflected in the contents of this file. However, when the **E2E View** window displays application details, the information about JP1 events in the **JP1Event** tab are displayed with the contents of this file applied.

- Note on the aggregate results displayed in the event timeline in the **Event Analysis View** window

  The aggregate results before this file is applied are not reflected in the contents of this file.

6.2.5 Defining mapping target for JP1 events

JP1/OA maps JP1 events obtained from JP1/IM to applications according to the default mapping rule.

The default JP1/OA mapping rule is described as follows.

1. If the Product name (`E.PRODUCT_NAME`) of a JP1 event is `/HITACHI/JP1/AJS` or `/HITACHI/JP1/AJS2`, map to the application obtained from JP1/AJS3 - Manager.
2. If the Product name (`E.PRODUCT_NAME`) of a JP1 event is `/HITACHI/JP1/PFM/ALARM_EVENT`, `/PFM/ALARM_EVENT`, or `/HITACHI/JP1/PFM/STATE_EVENT`, map to the application obtained from JP1/PFM - Manager. When mapping to the application, use the Object ID (`E.OBJECT_ID`) to specify a PFM agent type.
3. If an Event sourcehost (`E.JP1_SOURCEHOST`) exists for a JP1 event, map to the host that match with `E.JP1_SOURCEHOST` managed by JP1/OA. If there is no host that match with `E.JP1_SOURCEHOST`, discard the JP1 event. #
4. If an Event sourcehost (`E.JP1_SOURCEHOST`) does not exist for a JP1 event, map to the host that match with `B.SOURCESERVER` (Event-issuing server name) managed by JP1/OA. If there is no host that match with `B.SOURCESERVER`, remove discard the JP1 event. #

#: If the host also matches with a mapping rule for the application defined in the custom collector, the mapping with the application takes priority. For details, see *6.4.4 Defining mapping target for JP1 events*.

If you want to change the mapping target for a JP1 event, you can specify the mapping target in the definition file for JP1 event mapping target.

When the definition file for JP1 event mapping target is created, and the contents of the definition file are applied to

JP1/OA, JP1 events obtained from JP1/IM are mapped to the applications based on the contents of the definition file. JP1 events that do not match with the contents of the definition file are mapped to the applications based on the JP1/OA default rule.

(1) Creating a definition file for JP1 event mapping targets

Use the following procedure to create a definition file (`eventMapping.conf`) that specifies mapping targets for JP1 events.

1. Create a definition file for JP1 event mapping targets.

For details about the definition file, see *(3) Format of the definition file for JP1 event mapping targets*.

2. Save the definition file.

For the file name and the file extension, specify `eventMapping.conf`.

Save the file with UTF-8 encoding.

(2) Registering the definition file for JP1 event mapping targets

This section describes how to register the created definition file for JP1 event mapping targets to JP1/OA.

1. Place the definition file for JP1 event mapping targets in JP1/OA.

Place the created definition file for JP1 event mapping targets in the following folders.

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

2. Apply the definition file for JP1 event mapping targets to JP1/OA.

After this definition file is saved, it will be read automatically when any of the following operations is performed:

- The next time that events are collected
- When the **E2E View** window displays application details
- When the **Event Analysis View** window collects event details

(3) Format of the definition file for JP1 event mapping targets

This section describes the file which defines the mapping targets for JP1 events.

Format

host-name-of-the-mapping-target, *host-name-of-the-collector*, *product-name-of-the-collector*
{
event-condition
:
OR
event-condition
:
EXCLUDE
event-condition
:
}
host-name-2-of-the-mapping-target, *host-name-2-of-the-collector*, *product-name-2-of-the-collector*
{
event-condition
:
OR
event-condition
:
EXCLUDE
event-condition
:
}
:
:

File

`eventMapping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\conf`

For cluster systems:

shared-folder-name`\Analytics\conf`

When the definitions are applied

After this definition file is saved, it will be read when any of the following operations is performed:

- The next time that events are collected
- When the **E2E View** window displays application details
- When the **Event Analysis View** window collects event details

Description

The definition file specifies conditions for JP1 events to be mapped for each of the application specified by Resource ID, Parent Resource ID, and Parent Resource Type.

Note the following when specifying the definition file.

- Lines beginning with hash mark "#" are treated as comment lines.
- Blank lines are ignored.
- The entries are case sensitive.

Setting items

Items to define are described in the table below.

Setting item	Description	Setting value	Location in the JP1/OA window to check the setting value
Resource ID	Host name or service ID of the application to be mapped	- Host name for JP1/Base, JP1/AJS3 - Manager, or JP1/AJS3 - Agent - Service ID for JP1/PFM - Agent	From the **E2E View** window, select the application, and then click **Show Detail** to display the application details window. In that window, click the **Basic Information** tab.#
Parent Resource ID	IP address or host name of the collector for the application to be mapped	IP address or host name of JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	In the **IP Address/Host Name** column in the **Application** tab in the **Management Tool Registration** window.
Parent Resource Type	Product name of the collector for the application to be mapped	Product name (`JP1/IM - Manager`, `JP1/AJS3 - Manager`, or `JP1/PFM - Manager`)	The **Product Name** column in the **Application** tab in the **Management Tool Registration** window.

Setting item	Description	Setting value	Location in the JP1/OA window to check the setting value
Event condition	Conditions for JP1 events that you want to map	Specify the event condition following the same procedure as that of definition file for JP1 events to be obtained from JP1/IM. For details about event conditions to be specified, see *6.2.4 (3) Format of the definition file for JP1 events to be obtained from JP1/IM*.	--

(Legend) --: Not applicable

#: Host names for JP1/Base and JP1/AJS3 are displayed under the **Name** column in the detail window. The JP1/PFM service ID is displayed in the **Service ID** column of the details window.

Example definition

The following example maps a JP1 event to `AgtHost01` collected from `JP1/AJS3 - Manager` (Host name: `AJSM#01`) when the event ID is `101` or `102`, the severity level is Error, and the name of the server that issued the event is `host3`.

```
AgtHost01,AJSM#01,JP1/AJS3 - Manager
{
B.ID IN 101 102
E.SEVERITY IN Error
B.SOURCESERVER IN host3
}
```

Notes

- Note on the status of errors and warnings displayed for applications in the **E2E View** window

  The status of errors and warnings before this file is applied are not reflected in the contents of this file. However, when the **E2E View** window displays application details, the information about JP1 events in the **JP1Event** tab are displayed with the contents of this file applied.

- Note on the aggregate results displayed in the event timeline in the **Event Analysis View** window

  The aggregate results before this file is applied are not reflected in the contents of this file.

6.3 Registering a custom collector and specifying settings for monitoring an application

To manage an IT infrastructure system that includes an application (a custom application), such as a third-party product, you need to register a collector (a custom collector) by using the definition file. In this collector, you need to specify information about the applications to be monitored.

By periodically updating the definition file with the application information specified, you can also monitor the application periodically. JP1/OA provides a sample of a collector that obtains information managed by Zabbix. For more details, see *Appendix I. How to Use sample collectors.*

6.3.1 Defining a collector

To obtain information about applications, such as third-party products, you need to define a separate collector for each of the target applications.

(1) Creating a collector definition file

Use the following procedure to create a definition file (`CollectorMeta.conf`) that defines a collector.

1. Create a collector definition file.
For details about the definition file, see *(3) Format of the collector definition file.*

2. Save the definition file.
Specify `CollectorMeta.conf` as the file name and extension.
Save the file with UTF-8 encoding.

(2) Registering collector definition file

Register the created collector definition file in JP1/OA.

1. Create a collector folder under the following paths.

For non-cluster systems:
installation-destination-folder-of-JP1/OA`\lib\collector\application`
For cluster systems:
shared-folder-name`\Analytics\lib\collector\application`

Note the following points when you create a folder:
- Create a folder for each application.
- Give a unique name to the folder because the folder name is recognized as the collector name. Do not change the folder name after you run the `reloadproperty` command in step 3.

- The folder name must be from 1 to 64 characters. The following characters cannot be used:
  Double quotation marks (`"`), asterisks (`*`), commas (`,`), slashes (`/`), colons (`:`), semicolons (`;`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), vertical bars (`|`), backslash (`\`)

2. Place the collector definition file in the collector folder.

Place the collector files in the collector folder that you created.

3. Apply the collector definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the collector definition file to JP1/OA.

4. Confirm that the contents of the collector definition file have been applied.

Display the **Custom** tab in the **Management Tool Registration** window, and verify that the collector has been added.

(3) Format of the collector definition file

This file is used for defining a collector.

Format

Specification-key-name=setting-value

File

`CollectorMeta.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collector-folder***

For cluster systems:

shared-folder-name`\Analytics\lib\collector\application\`***collector-folder***

Definition application timing

The `reloadproperty` command is executed.

Content to be specified

Specify each key name and value on a single line.

Note the following when specifying settings in a definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.

- Definitions are case-sensitive.

Settings

Items to define are described in the table below.

Key name	Setting description	Setting value	Optional or required	Location to which the definition is applied.
format.version	Specify the version of the collector format.	0001 (fixed)	Required	--
collector.productName	Specify the product name to be managed by the collector.	255 or fewer characters (except control characters)	Optional	The **Product Name** column of the **Custom** tab in the **Management Tool Registration** window
collector.providerName	Specify information about the provider of the collector.	255 or fewer characters (except control characters)	Optional	The **Provider Name** column of the **Custom** tab in the **Management Tool Registration** window
collector.version	Specify the collector version.	128 or fewer characters (except control characters)	Optional	--

(Legend) --: Not applicable

6.3.2 Defining an application

You can define information about applications to be monitored by registering a custom collector.

(1) Creating an application definition file

Use the following procedure to create a definition file (`customApplication.conf`) that defines information about an application.

1. Create an application definition file in CSV format.
For details about the definition file, see *(3)* Format of the application definition file.

2. Save the definition file.

Specify `customApplication.conf` as the file name and extension.

Save the file with UTF-8 encoding.

(2) Registering the application definition file

Register the created application definition file in JP1/OA.

1. Create a folder to store the definition file as follows:

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***\conf

For cluster systems:

shared-folder-name*Analytics*\lib\collector\application***collector-folder***\conf

2. Place the application definition file in the conf folder.

Place the application definition file in the `conf` folder that you created.

3. Apply the application definition file to JP1/OA.

The definition file will be loaded at the following times after the definition file has been saved:

- The next time configuration information is collected.
- When the user clicks the **Refresh Data** button in the **Custom** tab of the **Management Tool Registration** window.

(3) Format of the application definition file

This file is used to define an application.

Format

#UpdateTime, *date-and-time-when-the-definition-is-updated*
application-type, *application-name*, *name-of-host-on-which-application-is-operating*, *description-of-application*

:

File

`customApplication.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***\conf

For cluster systems:

shared-folder-name*Analytics*\lib\collector\application***collector-folder***\conf

Definition application timing

The definition file will be loaded at the following times after the definition file has been saved:

- The next time configuration information is collected.
- When the user clicks the **Refresh Data** button in the **Custom** tab of the **Management Tool Registration** window.

Content to be specified

Specify, in CSV format, information about any application to be monitored by JP1/OA.

Note the following when specifying settings in a definition file:

- The settings consist of a header part and a body part.
- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- Entries other than the host name are case sensitive.

Settings

Items to define are described in the table below.

Category	Column name	Description	Setting value	Optional or required	Location to which the definition is applied.
Header section (First row)	UpdateTime	date and time when the definition is updated	*YYYY-MM-DD*T*hh*:*mm*:*ss*.*mmm*TZD	Optional	The **Last Definition Updated** column in the list of collectors window displayed by selecting the **Custom** tab in the **Management Tool Registration** window.
Body section (Second row and after)	type	application type	64 or fewer characters (except control characters)	Required	The **Collector Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.

Category	Column name	Description	Setting value	Optional or required	Location to which the definition is applied.
	name	application name	255 or fewer ASCII characters (except control characters)	Required	The **Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
	hostname	name of host on which application is operating	255 or fewer ASCII characters (except control characters)	Required	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
	description	description of application	1,024 or fewer ASCII characters (except control characters)	Optional	The **Description** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.

Definition example

The following is an example of defining Zabbix and MySQL as items to be monitored:

```
#UpdateTime,2017-08-04T12:10:00.775+0900
App Zabbix Server,Zabbix server,zabbix host1,zabbix
App MySQL,Zabbix mysql,zabbix mysql host1,zabbix mysql
```

Notes

If the same name and hostname are defined for multiple applications in the same collector, the applications are recognized as being the same. However, if a value for the type is changed, the application before the change that was registered will be delected, and the value after the change will be registered as a new application.

6.4 Customize the monitoring of applications registered in a custom collector

Customizing the associations with each application makes it easier to understand and analyze the configuration of your IT infrastructure system. If the application to be monitored is defined in a custom collector, customization must be performed per collector.

6.4.1 Mapping between applications

When an application defined in a custom collector and its related applications are associated with each other, the **E2E View** window displays the associations between the applications. A definition file is used to define associations between applications.

(1) Creating application mapping definition files

Use the following procedure to create a definition file (`customAppMapping.conf`) that associates applications with each other.

1. Create application mapping definition files in CSV format.
For details about the definition file, see *(3) Format of application mapping definition files*.

2. Save the definition file.

Specify `customAppMapping.conf` as the file name and extension.

Save the file with UTF-8 encoding.

(2) Registering application mapping definition files

Register the created application mapping definition files in JP1/OA.

1. Place application mapping definition files in JP1/OA.

Place the created application mapping definition files in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***\conf

For cluster systems:

shared-folder-name\Analytics\lib\collector\application***collector-folder***\conf

2. Apply the application mapping definition files to JP1/OA.

After this definition file is saved, it will be read automatically the next time when **E2E View** window be displayed.

3. Confirm that the content of the application mapping definition files has been applied.

Display the **E2E View** window, and confirm that the icons of the hosts associated with the application used as the base point are highlighted, or that the icons of the hosts for which you want to remove the association with the application used as the base point are not highlighted.

(3) Format of application mapping definition files

This file defines the mapping between applications.

Format

#Resource ID,Resource Host,Related Resource ID,Related Resource Host,Related Parent Resource ID,Related Parent Resource Type,Type

application-name, host-name, application-name-of-mapping-target, host-name-of-mapping-target, host-name of-collector-of-mapping-target, product-name-of-collector-of-mapping-target, type

:

File

`customAppMapping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collector-folder***`\conf`

For cluster systems:

shared-folder-name`\`*`Analytics`*`\lib\collector\application\`***collector-folder***`\conf`

Definition application timing

The next time the **E2E View** window is displayed after this definition file is saved.

Content to be specified

In CSV format, specify the information about the applications for which you want to add or remove associations.

Note the following when specifying settings in a definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- The entries are case sensitive.

Settings

Items to define are described in the table below. If the applications for which mapping is to be defined have already been registered in JP1/OA, you can check the details of values to be specified for each column in the JP1/OA window.

Column name	Description	Setting values	Location in the JP1/OA window to check the setting value
ResourceID	Name of the application for which you want to specify an association	Application name	The **Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Resource Host	Host name of the application for which you want to specify an association	Name of host on which application is operating	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Related Resource ID	Information to identify the application for which you want to add or remove the association with the application specified in ResourceID	- Host name for JP1/Base, JP1/AJS3 - Manager, or JP1/AJS3 - Agent - Service ID for JP1/PFM - Agent - Application name if an application is defined in a custom collector	From the **E2E View** window, select the application, and then click **Show Detail** to display the application details window. In that window, click the **Basic Information** tab.#
Related Resource Host	Host name of the application for which you want to add or remove an association. This application was specified in ResourceID. (Specify this value only when associating with an application defined in a custom collector.)	Name of host on which application is operating	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.

Column name	Description	Setting values	Location in the JP1/OA window to check the setting value
Related Parent Resource ID	Information to identify the collector of the application for which you want to add or remove the association with the application specified in ResourceID	IP address or host name of JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	The **IP Address/Host Name** column in the **Application** tab in the **Management Tool Registration** window
		Collector name if an application is defined in the custom collector	The **Collector Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Related Parent Resource Type	Type of the collector for the application for which you want to add or remove an association. This application was specified in ResourceID.	Product name of JP1/IM - Manager, JP1/AJS3 - Manager, or JP1/PFM - Manager	The **Product Name** column in the **Application** tab in the **Management Tool Registration** window
		`Customized Application - Manager` (fixed) if an application is defined in the custom collector	--
Type	Type of operation (add or remove)	- Specify `Add` to add an association. - Specify `Remove` to remove an existing association.	--

(Legend) --: Not applicable

#: The host names for JP1/Base and JP1/AJS3, and the names of applications are displayed in the **Name** column of the detailed window. The JP1/PFM service ID is displayed in the **Service ID** column in the detailed window.

Definition example

The following example shows what to input to define the following content:

Definition example 1:

Add an association between a Zabbix server (Host name: `zabbix host1`) and JP1/AJS3 - Manager (Host name: `AgtHost01`).

The IP address for JP1/AJS3 - Manager is `192.168.10.10`.

Definition example 2:

Add an association between a Zabbix server (Host name: `zabbix host1`) and Zabbix mysql (Host name: `zabbix mysql host1`).

The collector for Zabbix mysql is `ZabbixManager01`.

Input example:

```
#Resource ID,Resource Host,Related Resource ID,Related Resource Host,Related Parent Resource ID,Related Parent Resource Type,Type
Zabbix server,zabbix host1,AgtHost01,,192.168.10.10,JP1/AJS3 - Manager,Add
Zabbix server,zabbix host1,Zabbix mysql,zabbix mysql host1,ZabbixManager01,Customized Application - Manager,Add
```

6.4.2 Mapping between applications and hosts

To associate or disassociate an application defined in a custom collector with a host managed by JP1/OA, you can add or remove the mapping between the application and the host by using the mapping definition file, which is used to associate or disassociate applications with or from hosts.

You can use the application-host mapping definition file for the following purposes:

- To add or remove an association between an application and a host

  For example, if multiple hosts with the same name exist and unnecessary associations are automatically made, you can use the definition file to remove the unnecessary associations.

  To add the associations, in the definition file specify `Add` for Type. To remove the associations, in the definition file specify `Remove` for Type.

- To specify that the host names obtained from applications are to be regarded as the host names managed by JP1/OA

  For example, if the host name obtained from an application is different from the host name managed by JP1/OA, the application and the host cannot be associated automatically. In such a case, use the definition file to specify that the host name obtained from the application is to be regarded as the host name managed by JP1/OA. This enables you to associate the application and the host.

  To specify that the obtained host name is to be regarded as the host name managed by JP1/OA, in the definition file specify `RegardAs` for Type.

Note that applications will belong to the same consumers as those to which automatically-associated hosts belong. Therefore, if you change the associations between the applications and hosts, the consumers to which the applications belong might change depending on the associated hosts.

(1) Creating an application-host mapping definition file

Use the following procedure to create a definition file (`customAppHostMapping.conf`) that associates or disassociates applications and hosts:

1. Create an application-host mapping definition file in CSV format.

For details about the definition file, see *(3) Format of the application-host mapping definition file*.

2. Save the definition file.

Specify `customAppHostMapping.conf` as the file name and extension.

Save the file with UTF-8 encoding.

(2) Registering the application-host mapping definition file

Register the created application-host mapping definition file in JP1/OA.

1. Place the application-host mapping definition file in JP1/OA.

Place the created application-host mapping definition file in the following folder:

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collector-folder***`\conf`

For cluster systems:

shared-folder-name`\Analytics\lib\collector\application\`***collector-folder***`\conf`

2. Apply the application-host mapping definition file to JP1/OA.

Use the `reloadproperty` command to apply the contents of the application-host mapping definition file to JP1/OA.

Alternatively, you can restart the JP1/OA service to load all the contents of the application-host mapping definition file.

3. Confirm that the contents of the application-host mapping definition file have been applied.

Display the **E2E View** window, and confirm that the icons of the hosts associated with the application used as the base point are highlighted, or that the icons of the hosts for which you want to remove the association with the application used as the base point are not highlighted.

(3) Format of the application-host mapping definition file

This file defines the mapping between applications and hosts.

Format

#App Resource ID, App Host Name, Regarded Host Name/Host Resource ID, Type

application-name, host-name, host-name-managed-by-JP1/OA, type

:

File

`customAppHostMapping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collector-folder***`\conf`

For cluster systems:

shared-folder-name`\`*`Analytics`*`\lib\collector\application\`***collector-folder***`\conf`

Definition application timing

When JP1/OA is started or the `reloadproperty` command is executed.

Content to be specified

In CSV format, specify the information about the applications and hosts for which you want to add or remove associations.

Note the following when specifying settings in a definition file:

- A line starting with # is treated as a comment line.
- Blank lines are ignored.
- The entries are case sensitive.

Settings

Items to define are described in the table below. If the applications for which mapping is to be defined have already been registered in JP1/OA, you can also check the details of the settings to be specified for each column in the JP1/OA window.

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
App Resource ID	Name of the application for which you want to specify an association	Application name	The **Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
App Host Name	Host name of the application for which you want to specify an association	Name of host on which application is operating	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Regarded Host Name/ Host Resource ID	Name of the host to be associated you want to associate with the host name obtained from the application, or ID of the host to be associated with or disassociated from the application	If you want to add or remove an association between an application and a host (by specifying `Add` or `Remove` in Type), specify the ID of a host managed by JP1/OA.	The **ID** column of the output results of the `listresources` command.
		If you want the host name obtained from the application to be regarded as the host name managed by JP1/OA (by specifying `RegardAs` in Type), specify the host name managed by JP1/OA.	The **Host Name** column in the **Basic Information** tab in the virtual machine details or host details window. To display the virtual machine details or host details window, from the **E2E View** window, select the virtual machine or host, and then click **Show Detail**.

Column name	Description	Setting value	Location in the JP1/OA window to check the setting value
Type	Type	- Specify `Add` to add an association between applications and hosts. - Specify `Remove` to remove the association between applications and hosts. - Specify `RegardAs` if you want the host name obtained from the application to be regarded as the host name managed by JP1/OA.	--

(Legend) --: Not applicable

Definition example

The following shows an example of adding an association between a Zabbix server (Host name: `zabbix host1`) and the host (ID: `vm2`) managed by JP1/OA:

```
#App Resource ID,App Host Name,Regarded Host Name/Host Resource ID,Type
Zabbix server,zabbix host1,vm2,Add
```

6.4.3 Defining a grouping of applications

In JP1/OA, the **E2E View** window and **Dashboard** window display associated applications that are defined in a custom collector, in groups, according to the contents defined in the definition file.

Specify types of applications in the definition file. Applications whose types are not defined in the definition file are grouped and are displayed in **Other Applications**.

(1) Creating a definition file for grouping applications

Use the following procedure to create a definition file (`customAppGrouping.conf`) that defines a group of associated applications:

1. Create a definition file for grouping applications.

For details about the definition file, see *(3) Format of the definition file for grouping applications*.

If you want to display application groups of your choice in the **Dashboard** window, you need to edit the definition file for grouping applications (`appGrouping.conf`). Specify the group names defined in the `customAppGrouping.conf`. For details, see 6.2.3 *(3) Format of the definition file for grouping applications*.

2. Save the definition file.

Specify `customAppGrouping.conf` as the file name and extension.

Save the file with UTF-8 encoding.

(2) Registering the definition file for grouping applications

Use the following procedure to apply the created definition file for grouping applications to JP1/OA:

1. Place the definition file for grouping applications in JP1/OA.

Place the created definition file for grouping applications in one of the following folders:

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***\conf

For cluster systems:

shared-folder-name\Analytics\lib\collector\application***collector-folder***\conf

2. Confirm that the contents of the definition file for grouping applications have been applied.

Display the **E2E View** window, and confirm that the applications displayed in the application area are grouped according to the edited definitions.

If you edited the definition file for grouping applications (`appGrouping.conf`) in step 1, confirm, in the **Dashboard** window, that the top three groups defined in `appGrouping.conf` are displayed in the application summary in the System Status Summary for Application Administrators report.

(3) Format of the definition file for grouping applications

Application grouping definition files are used to define a grouping of applications.

Format

group-name-1
{
application-type-1
application-type-2
:
:
}
group-name-2
{
application-type-3
application-type-4
:
:
}
:
:

File

`customAppGrouping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collector-folder***`\conf`

For cluster systems:

shared-folder-name`\`*`Analytics`*`\lib\collector\application\`***collector-folder***`\conf`

When the definitions are applied

The next time the **E2E View** window or **Dashboard** window is displayed after this definition file is saved.

Description

The definition file specifies the group name and the types of applications that will belong to the group for each group.

Note the following when specifying the definition file:

- Lines beginning with a hash mark (#) are treated as comment lines.
- Blank lines are ignored.

- Alphabetic characters are case sensitive.

Setting items

1. Group name

Specify the name for identifying the group.

Specify the group name by using 128 or fewer characters.

2. Application type

Specify the type of applications that will belong to the group.

Define the types of applications in the application definition file (`customApplication.conf`).

Definition example

The following is an example of defining multiple applications as a group in a Zabbix group:

```
Zabbix
{
App FTP Service
App HTTP Service
App HTTPS Service
App IMAP Service
App LDAP Service
App MySQL
App NNTP Service
App NTP Service
App POP Service
App SMTP Service
App SSH Service
App Telnet Service
App Zabbix Agent
App Zabbix Proxy
App Zabbix Server
ICMP Ping
IPMI Intel SR1530
IPMI Intel SR1630
JMX Generic
JMX Tomcat
OS AIX
OS FreeBSD
OS HP-UX
OS Linux
OS Mac OS X
OS OpenBSD
OS Solaris
OS Windows
SNMP Device
SNMP Disks
SNMP Generic
SNMP Interfaces
SNMP OS Linux
SNMP OS Windows
SNMP Processors
Virt VMware
Virt VMware Guest
Virt VMware Hypervisor
}
```

6.4.4 Defining mapping target for JP1 events

JP1/OA maps JP1 events obtained from JP1/IM to applications according to the default mapping rule.

The default JP1/OA mapping rule is shown below. Note that when all of the conditions are met, JP1 events are

mapped to the applications defined in the custom collector.
- The Object ID (`E.OBJECT_ID`) for a JP1 event matches with an application name.
- The Event sourcehost (`E.JP1_SOURCEHOST`) for a JP1 event matches with the host name of an application.

If you want to change the mapping target for a JP1 event, you can specify the mapping target in the definition file for JP1 event mapping target.
When the definition file for JP1 event mapping target is created, and the contents of the definition file are applied to JP1/OA, JP1 events obtained from JP1/IM are mapped to the applications based on the contents of the definition file. JP1 events that do not match with the contents of the definition file are mapped to the applications based on the JP1/OA default rule.

(1) Creating a definition file for JP1 event mapping targets

Use the following procedure to create a definition file (`customEventMapping.conf`) that specifies mapping targets for JP1 events.

1. Create a definition file for JP1 event mapping targets.

For details about the definition file, see *(3) Format of the definition file for JP1 event mapping targets*.

2. Save the definition file.

For the file name and the file extension, specify `customEventMapping.conf`.

Save the file with UTF-8 encoding.

(2) Registering the definition file for JP1 event mapping targets

This section describes how to register the created definition file for JP1 event mapping targets to JP1/OA.

1. Place the definition file for JP1 event mapping targets in JP1/OA.

Place the created definition file for JP1 event mapping targets in the following folders.

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***\conf

For cluster systems:

shared-folder-name\Analytics\lib\collector\application***collector-folder***\conf

2. Apply the definition file for JP1 event mapping targets to JP1/OA.

After this definition file is saved, it will be read automatically when any of the following operations is performed:
- The next time that events are collected
- When the **E2E View** window displays application details

- When the **Event Analysis View** window collects event details

(3) Format of the definition file for JP1 event mapping targets

This section describes the file which defines the mapping targets for JP1 events.

Format

Application-name-of-the-mapping-target, *host-name-of-the-mapping-target*
{
event-condition
:
OR
event-condition
:
EXCLUDE
event-condition
:
}
Application-name-2-of-the-mapping-target, *host-name-2-of-the-mapping-target*
{
event-condition
:
OR
event-condition
:
EXCLUDE
event-condition
:
}
:
:

File

`customEventMapping.conf`

Save the file with UTF-8 encoding.

Storage directory

For non-cluster systems:

installation-destination-folder-of-JP1/OA`\lib\collector\application\`***collect***

or-folder\conf

For cluster systems:

shared-folder-name*Analytics*\lib\collector\application***collector-folder***\conf

When the definitions are applied

After this definition file is saved, it will be read automatically when any of the following operations is performed:

- The next time that events are collected
- When the **E2E View** window displays application details
- When the **Event Analysis View** window collects event details

Description

The definition file specifies conditions for JP1 events to be mapped for each of the application specified by Resource ID, and Resource Host.

Note the following when specifying the definition file.

- Lines beginning with hash mark "#" are treated as comment lines.
- Blank lines are ignored.
- The entries are case sensitive.

Setting items

Items to define are described in the table below.

Setting item	Description	Setting value	Location in the JP1/OA window to check the setting value
Resource ID	Name of the application to be mapped	Application name	The **Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.

Setting item	Description	Setting value	Location in the JP1/OA window to check the setting value
Resource Host	Host name of the application to be mapped	Name of host on which application is operating	The **Host Name** column in the **Basic Information** tab in the application details window. To display the application details window, from the **E2E View** window, select the application, and then click **Show Detail**.
Event condition	Conditions for JP1 events that you want to map	Specify the event condition following the same procedure as that of definition file for JP1 events to be obtained from JP1/IM. For details about event conditions to be specified, see *6.4.4 (3) Format of the definition file for JP1 event mapping targets*.	--

(Legend) --: Not applicable

Example definition

The following example maps a JP1 event to a Zabbix server (Host name: `zabbix host1`) when the event ID is `103` or `104`, the severity level is Error, and the name of the server that issued the event is `host3`.

```
Zabbix server, zabbix host1
{
B.ID IN 103 104
E.SEVERITY IN Error
B.SOURCESERVER IN host3
}
```

Notes

- Note on the status of errors and warnings displayed for applications in the **E2E View** window

  The status of errors and warnings before this file is applied are not reflected in the contents of this file. However, when the **E2E View** window displays application details, the information about JP1 events in the **JP1Event** tab are displayed with the contents of this file applied.

- Note on the aggregate results displayed in the event timeline in the **Event Analysis View** window

  The aggregate results before this file is applied are not reflected in the contents of this file.

6.5 End monitoring of an application by deleting a custom collector

To end monitoring of an application in JP1/OA, delete the collectors that have definition information about the application.

1. Delete the collector folder for the application for which you want to end monitoring.

For non-cluster systems:

installation-destination-folder-of-JP1/OA\lib\collector\application***collector-folder***

For cluster systems:

shared-folder-name\Analytics\lib\collector\application***collector-folder***

2. Apply information about the deleted application to JP1/OA.

You can apply information about the deleted application to JP1/OA by using the `reloadproperty` command.

3. Confirm that the collector has been deleted.

Display the **Custom** tab in the **Management Tool Registration** window and confirm that the collector has been deleted.

7.Commands
7.1 Command list

The following table lists command that you can use in JP1/OA.

Table 7-1 Building-related commands

Command name	Functionality	Refer to:
encryptpassword (creates a password file)	Creates a password file used to specify arguments for commands.	7.6.1
hcmds64checkauth (checks connections with an external authentication server)	Checks the settings of the configuration file for linking with external authentication servers, and checks the connection with an external authentication server, when connecting with the external server.	7.6.2
hcmds64fwcancel (registers an exception for the Windows firewall)	Registers an exception so that communication between the JP1/OA server and the web browser is not blocked by the Windows firewall.	7.6.3
hcmds64intg (deletes authentication data and confirms the deletion)	Deletes authentication data registered in the repository of the server that manages user accounts. The command also displays the address of the server in which the authentication data is registered. If you fail to delete authentication data when uninstalling JP1/OA, use this command to delete the authentication data.	7.6.4
hcmds64ssltool (creates a private key and self-signed certificate)	Creates private keys, CSRs, and the self-signed certificate (including its content files), which are required for SSL connections.	7.6.5
hcmds64checkcerts (checks the expiration date of the SSL server certificate)	Checks the expiration date of the SSL server certificate specified in the `user_httpsd.conf` file when an HTTPS connection is used between JP1/OA and the Web browser.	7.6.6

Table 7-2 Operation-related commands

Command name	Functionality	Refer to:
addconsumers (creates consumers)	Creates a consumer for JP1/OA.	7.7.1
addsetting (creates configuration information)	Creates configuration information (retrieval ranges, authentication information, collectors, threshold profiles, and consumers) for JP1/OA.	7.7.2

Command name	Functionality	Refer to:
deletesetting (deletes configuration information)	Deletes configuration information (retrieval ranges, authentication information, collectors, threshold profiles, and consumers) for JP1/OA.	7.7.3
disablemonitoring (stops the monitoring status)	Invalidates the monitoring status of resources managed in JP1/OA.	7.7.4
enablemonitoring (executes monitoring)	Validates the monitoring status of resources managed in JP1/OA.	7.7.5
getsettings (obtains configuration information)	Obtains configuration information (retrieval ranges, authentication information, collectors, threshold profiles, and consumers) for JP1/OA.	7.7.6
hcmds64srv (starts, stops, or displays the status of JP1/OA)	Starts or stops JP1/OA services and databases. The command also displays the status of JP1/OA services.	7.7.7
hcmds64unlockaccount (unlocks a user account)	Unlocks a user account. Use this command when you cannot log in to JP1/OA because all the user accounts are locked.	7.7.8
hcmds64chgurl (changes the URL for JP1/OA)	Changes the URL for accessing the JP1/OA server when settings such as the host name, IP address, or port number for the JP1/OA server are changed.	7.7.9
listconsumers (obtains the list of consumers)	Outputs the list of JP1/OA consumers.	7.7.10
listresources (lists resource information)	Lists resource information managed by JP1/OA.	7.7.11
outputevent (outputs event information to a CSV file)	Outputs event information managed by JP1/OA to a CSV file.	7.7.12
outputlatestperf (outputs performance information (latest value) to a CSV file)	Outputs performance information (the most recent values) for the resources managed by JP1/OA to a CSV file.	7.7.13
outputresource (outputs resource information to a CSV file)	Outputs resource information or a list of related resources managed by JP1/OA to a CSV file.	7.7.14
outputtimeseriesperf (outputs performance information, in chronological order, to a CSV file)	Outputs performance information (in chronological order) for the resources managed by JP1/OA to a CSV file.	7.7.15
reloadproperty (re-reads the definition file)	Reloads the following definition file. - Definition files for linking with JP1/SS or JP1/NP. - Definition files for setting up templates for the commands to be executed in Execute Action window. - Definition files for mapping between applications and hosts. - Collector definition files for monitoring applications.	7.7.16

Command name	Functionality	Refer to:
updatecredentials (edits authentication information)	Edits authentication information for the resources managed by JP1/OA.	7.7.17
updatesetting (edits configuration information)	Edits configuration information (retrieval ranges, authentication information, collectors, threshold profiles, and consumers) for JP1/OA.	7.7.18

Table 7-3 Maintenance-related commands

Command name	Functionality	Refer to:
backupsystem (backs up the JP1/OA system)	Backs up JP1/OA configuration information or database information in the folder you specify.	7.8.1
expandretention (extends the retention period for performance information)	Extends the retention period for performance information retained by JP1/OA.	7.8.2
hcmds64getlogs (collects log information)	Collects log information that is output during operation of JP1/OA, and outputs the log information to an archive file.	7.8.3
joanodecount (displays the number of management nodes)	Displays the number of management nodes in JP1/OA.	7.8.4
restoresystem (restores the JP1/OA system)	Restores the backup for JP1/OA settings or database information data that you acquired by executing the backupsystem command.	7.8.5

7.2 Notes on the use of commands

- If the command to be executed in an environment where User Account Control (UAC) of Windows is valid requires the Administrator permission, execute the command from the administrator console of JP1/OA.

To start the administrator console:

For Windows Server 2008

1. In the **Start** menu, select **All Program**, **JP1_Operations Analytics**, and then **Analytics Command**.

For Windows Server 2012

1. From Desktop, display the Start Screen.
2. Right-click the Start Screen to display **All Applications**.
3. In the **JP1_Operations Analytics** folder, select **Analytics Command**.

For Windows Server 2016

1. Open the Start menu.
2. In the **JP1_Operations Analytics** folder, select **Analytics Command**.

To stop the administrator console:

In the command prompt, either enter the exit command or click the **Close** button (×).

- If you enable **Quick Edit Mode** in the command prompt, and then click the mouse on the screen, the screen output is stopped until the quick edit mode is canceled. Therefore, we recommend that you do not use the quick edit mode.

- To interrupt command execution, press **Ctrl** and **C** at the same time. If you interrupt command execution, make sure that you read the message issued at the interruption of the command to check for any problems. If necessary, re-execute the command. If you interrupt execution of a command, the return value might become undefined.

- When using commands in a cluster environment, execute them on the active host. However, the hcmds64getlogs command can also be executed on the standby host.

7.3 Command coding format

This section explains the command coding format.

The following items are explained for each command. However, some items are not explained, depending on the command.

Functionality

Describes the command functionality.

Format

Describes the specification format of the command in the following format:

Command name [[/option[value]...]

A combination of /option and value is called an *option*. Options of each command are collectively called *arguments*.

Arguments

Describes the arguments for the command.

Storage location

Describes the storage location for the command.

Execution permissions

Describes the permissions required for executing the command.

Notes

Provides notes on execution of the command.

Return values

Describes the return values of the command.

Example

Provides an example of usage of the command.

7.4 Characters usable for command arguments

You can specify the following characters for command arguments:

- The specification method for command arguments must comply with the specifications of the OS command prompt or shell. Therefore, if an argument value contains a space ( ) or special symbols, you need to escape such characters, for example, by enclosing each of the characters with double quotation marks (").

- You can use the following types of characters when specifying a path with an argument of a command:
  Alphanumeric characters, underscores (_), periods (.), hyphens (-), spaces ( ), left parentheses (( ), right parentheses ( )), hash marks (#), at marks (@), colons (:), and backslash (\)

- You can use a colon only as a drive delimiter.

- You can use a backslash only as a folder delimiter.

- When specifying a path in an argument, you cannot use a path in UNC format.

- When specifying a path in an argument, you cannot use a path that has a folder name that begins or ends with a space or a folder name that consists of only spaces.

- When specifying a path in an argument, you cannot use a path that has a folder name that begins or ends with a period or consists of only periods.

- Unless otherwise stated, the path length is from 1 to 230 characters in the absolute path.

- Unless otherwise stated, each command argument is case sensitive.

- Do not specify the following names as a file name or folder name because these names are reserved words for the OS:
CON, PRN, AUX, CLOCK$, NUL, COM0, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT0, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, and LPT9

7.5 Overview of using commands to perform operations for JP1/OA configuration information

In JP1/OA, you can perform operations (add, obtain, edit, and delete) for the following settings that are required to manage resources:

- Search ranges
- Authentication information
- Collectors
- Threshold profiles
- Consumers

The following describes the commands to be used for individual operations.

Add

Create a JSON file that includes configuration information, and then execute the `addsetting` command.
When adding configuration information for a search range, authentication information, a collector, or a consumer, create a JSON file by referencing the template files that were stored at the time of installation. When creating configuration information for a threshold profile, use the `getsettings` command to obtain the preset default profile, and then create a JSON file by referencing the file you obtained.

Obtain

Execute the `getsettings` command to output existing configuration information to a JSON file.

Edit

Based on the JSON file you obtained by using the `getsettings` command, write the information that you want to edit to another JSON file, and then execute the `updatesetting` command.

Delete

Execute the `deletesetting` command to delete the existing configuration information.

> Note:
> You can use commands that use CSV files to create or obtain a consumer, and to edit authentication information. For details about the commands, see *7.7.1 addconsumers (create consumers)*, *7.7.10 listconsumers (obtains the list of consumers)*, or *7.7.17 updatecredentials (edits authentication information)*.

To create a JSON file to be specified when executing the commands, refer to the template files and default profiles described in the tables below.

(1) Template files for search ranges

For details about the settings to be specified when creating the file, see the section describing how to create a search range in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update a search range.

Storage location of the template file	Template file name
installation-destination-folder-of-JP1/OA\sample\setting\IpAddrRange	Sample_Add_IpAddrRange.json

(2) Template files for authentication information

For details about the settings to be specified when creating the file, see the section describing how to create authentication information in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update authentication information.

Protocol	Storage location of the template file	Template file name
WMI	***installation-destination-folder-of-JP1/OA***\sample\setting\Credential	Sample_Add_Credential_WMI.json
SSH	***installation-destination-folder-of-JP1/OA***\sample\setting\Credential	Sample_Add_Credential_SSH.json
SNMPv1 or SNMPv2c	***installation-destination-folder-of-JP1/OA***\sample\setting\Credential	Sample_Add_Credential_SNMP.json
SNMPv3	***installation-destination-folder-of-JP1/OA***\sample\setting\Credential	Sample_Add_Credential_SNMPv3.json
SMI-S WBEM	***installation-destination-folder-of-JP1/OA***\sample\setting\Credential	Sample_Add_Credential_WBEM.json

(3) Template files for collectors

For details about the settings to be specified when creating the file, see the section describing how to create a collector in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update a collector.

Collector	Storage location of the template file	Template file name
JP1/IM - Manager	***installation-destination-folder-of-JP1/OA***\sample\setting\Consumer	For Windows: Sample_Add_Collector_App_IM_Win.json For UNIX: Sample_Add_Collector_App_IM_Unix.json
JP1/AJS3 - Manager	***installation-destination-folder-of-JP1/OA***\sample\setting\Consumer	For Windows: Sample_Add_Collector_App_AJS_Win.json For UNIX: Sample_Add_Collector_App_AJS_Unix.json
JP1/ PFM - Manager	***installation-destination-folder-of-JP1/OA***\sample\setting\Consumer	For Windows: Sample_Add_Collector_App_PFM_Win.json For UNIX: Sample_Add_Collector_App_PFM_Unix.json
vCenter	***installation-destination-folder-of-JP1/OA***\sample\setting\Consumer	Sample_Add_Collector_vCenter.json

(4) Default profiles for threshold values for user resources

For details about the settings to be specified when creating the file, see the section describing how to create a user profile in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update a user profile.

Resource type	Default profile name
Virtual machine	Default Profile for VM
Windows host	Default Profile for Windows
Linux/UNIX host	Default Profile for Linux/UNIX
Volume	Default Profile for Volume

(5) Default profiles for threshold values for system resources

For details about the settings to be specified when creating the file, see the section describing how to create a system profile in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update a system profile.

Resource type	Default profile name
ESX	Default Profile for ESX
Hyper-V	Default Profile for Hyper-V
IP Switch	Default Profile for IP Switch
FC Switch	Default Profile for FC Switch

(6) Template files for consumers

For details about the settings to be specified when creating the file, see the section describing how to create a consumer in the *JP1/Operations Analytics REST API Reference Guide*. For details about the settings to be specified when editing the file, see the section in the same manual describing how to update a consumer.

Storage location of the template file	Template file name
installation-destination-folder-of-JP1/OA\sample\setting\Consumer	Sample_Add_Consumer.json

7.6 Building-related commands

7.6.1 encryptpassword (creates a password file)

Functionality

This command creates a password file used to specify arguments for commands of JP1/OA.

You can create an encrypted password file by specifying, as arguments, the user ID and password of the user registered in JP1/OA and a path for the password file to be created.

Format

encryptpassword

/user ***user-ID***

/password ***password***

/passwordfile ***password-file***

Arguments

/user ***user-ID***

Specify the user ID of the JP1/OA user for whom you want to create a password file.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user ID is not case sensitive.

/password ***password***

Specify the user password that you specified in the user option.

You can specify from 1 to 256 characters.

Usable character types are the same as for the user option.

/passwordfile ***password-file***

Specify the path for the password file to be created, in absolute or relative path format. If the specified path already exists, an error occurs.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
4	An exclusive error occurred.
5	Communication failed.
6	Authentication failed (the specified value is invalid).
7	The specified path is invalid.
8	The output path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
200	Creation of a password file failed.
255	Command execution was interrupted due to an error other than above.

Example

The following example shows the use of this command to create a password file for the specified user:

```
encryptpassword /user user01 /password pass01 /passwordfile PasswordFilePath
```

7.6.2 hcmds64checkauth (checks connections with an external authentication server)

Functionality

This command checks the settings of the configuration file for linking with external authentication servers and also checks the connection with an external authentication server, when connecting with an external server.

JP1/OA can link with JP1/Base as an external authentication server.

This command checks the following items:

- The value of the key of the configuration file for linking with external authentication servers (exauth.properties), and which is shared when linking with an external authentication server
- Whether a correct value is set in the auth.server.type key of the configuration file for linking with external authentication servers (exauth.properties)

  Specify jp1base in the auth.server.type key. The entered value is case sensitive. If internal, which indicates the default of the auth.server.type key, is specified, an error message is displayed to indicate that the external server setting is not validated.
- Whether JP1/Base and the common component are on the same host
- Whether the version of JP1/Base is supported
- Whether JP1/Base users can be authenticated correctly

Format

hcmds64checkauth

/user ***user-name***

/pass ***password***

[/summary]

Arguments

/user ***user-name***

Specify the user name that has been registered in the external authentication server. However, make sure that the user name you specify does not overlap with one already registered in JP1/OA.

/pass ***password***

Specify the password that corresponds to the user name registered in the external authentication server.

/summary

Simplifies confirmation messages that are displayed when the command is executed. If you specify this option, possible displayed messages are those indicating success or failure of each processing phase, error messages, and messages indicating a processing result. Any error message that is the same as the message indicating a result is omitted.

Storage location

installation-destination-folder-of-common-component`/bin`

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1 to 99	Total number of syntax errors.
100	End code if the number of syntax errors exceeds 100.
101 to 199	One or more connection errors or authentication errors occurred. 1s digit: Number of connection errors 10s digit: Number of authentication errors The maximum value is 9 for each of the above. Even if more than nine errors occur, the value remains at 9.

Return value	Description
247	Authentication failed because the user ID specified in the user option overlaps with the user ID registered in JP1/OA. Specify a unique user ID.
248	JP1/Base is not installed on the host that executed the command.
249	The version of JP1/Base in use is not supported.
250	The command was executed from the secondary server.
252	The settings of common items for the definition file are invalid.
253	No external authentication linkage has been set.
254	The argument is invalid.
255	The command finished abnormally.

Example

The following example shows the use of this command to check connections with an external authentication server:

```
hcmds64checkauth /user test01 /pass TTdate00 /summary
```

7.6.3 hcmds64fwcancel (registers an exception for the Windows firewall)

Functionality

This command registers an exception so that communication between the JP1/OA server and the web browser is not blocked by the Windows firewall.

Format

hcmds64fwcancel

Storage location

installation-destination-folder-of-common-component\bin

Execution permissions

The Administrator permission is required to perform this operation.

Return values

This command has no return value. Therefore, to determine whether the processing finished normally, check whether HBase(Web) is correctly registered in the reception rules of the Windows firewall.

To check the Windows firewall, in Windows **Control Panel**, click **Windows Firewall**.

7.6.4 hcmds64intg (deletes authentication data and confirm the deletion)

Functionality

This command deletes authentication data registered in the repository of the server that manages user accounts. The command also displays the address of the server in which the authentication data is registered.

If you fail to delete authentication data when uninstalling JP1/OA, use this command to delete the authentication

data.

Format

hcmds64intg

{/delete /type Analytics | /print | /primary}

/user ***user-ID***

/pass ***password***

Arguments

/delete

Deletes authentication data.

/type Analytics

Specify Analytics as the product name of the server in which the authentication data is registered.

/print

Displays the name of the program in which the authentication data is registered.

/primary

Displays the host name or the IP address of the server in which the authentication data is registered.

/user ***user-ID***

Specify the user ID for connecting with the server in which the authentication data is registered. The user ID you specify must have the User Management permission.

/pass ***password***

Specifies the password of the account that has the User Management permission.

Storage location

installation-destination-folder-of-common-component`/bin`

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The authentication data has already been deleted.

Return value	Description
2	Authentication data is registered in the server on which you executed the command.
3	Authentication data is not registered in the server on which you executed the command.
4	Authentication data is not registered in the server on which you executed the command. In addition, an authentication error occurred on the server in which authentication data is registered.
253	An authentication error occurred on the server in which authentication data is registered.
254	Communication with the server in which authentication data is registered failed.
255	The command finished abnormally.

Example

The following example shows the use of this command to delete authentication data from the server that manages the user account:

```
hcmds64intg /delete /type Analytics /user user1 /pass pass1
```

7.6.5 hcmds64ssltool (creates a private key and self-signed certificate)

Functionality

This command creates private keys, CSRs, and self-signed certificate (including its content files), which are required for SSL connection.

When the `hcmds64ssltool` command is executed, files for the RSA cipher and Elliptic Curve Cryptography (ECC) are both output.

The created files are used for the following purposes:

- Submitting the CSR to a CA to acquire an SSL server certificate. You can build an SSL-connected environment by combining the acquired SSL server certificate and the private key.
- Building an SSL-connected environment by combining the self-signed certificate with the private key. However, we recommend that you use the environment for test purposes only because security intensity is low.
- Checking the details of the registration of the self-signed certificate from the content file of the self-signed certificate.

Format

hcmds64ssltool

[/key ***private-key-file-name***]

[/csr ***CSR-File-Name***]

[/cert ***self-signed-certificate-file-name***]

[/certtext ***name-of-content-file-of-self-signed-certificate***]

[/validity e***xpiry-date-of-self-signed-certificate***]

[/dname ***distinguished-name (DN)***]

[/sigalg ***signature-algorithm-for-server-certificate-for-RSA-cipher***]

[/eccsigalg ***signature-algorithm-for-server-certificate-for-elliptic-curve-cipher***]

[/ecckeysize ***keysize-of-private-key-for-elliptic-curve-cipher***]

Arguments

/key ***private-key-file-name***

Specify the path for storing the private key, in the absolute path format. Include the file name of the private key in the absolute path.

The private key for use with an RSA cipher is output with the specified file name. The private key for use with Elliptic Curve Cryptography is output with the `ecc-` prefix at the beginning of the file name.

If you omit this option, files named `httpsdkey.pem` and `ecc-httpsdkey.pem` are output to the default output destination path.

/csr ***CSR-File-Name***

Specify the path for storing the CSR, in the absolute path format. Include the CSR file name in the absolute path.

The CSR use with an RSA cipher is output with the specified file name. The CSR for use with Elliptic Curve Cryptography is output with the `ecc-` prefix at the beginning of the file name.

If you omit this option, files named `httpsd.csr` and `ecc-httpsd.csr` are output to the default output destination path.

/cert ***self-signed-certificate-file-name***

Specify the path for storing the self-signed certificate, in the absolute path format. Include the file name of the self-signed certificate in the absolute path.

The self-signed certificate use with an RSA cipher is output with the specified file name. The self-signed certificate for use with Elliptic Curve Cryptography is output with the `ecc-` prefix at the beginning of the file name.

If you omit this option, files named `httpsd.pem` and `ecc-httpsd.pem` are output to the default output destination path.

/certtext ***name-of-content-file-of-self-signed-certificate***

Outputs the content of the self-signed certificate in text format. Specify the path for storing the file, in the absolute path format. Include the text file name in the absolute path.

The content of the self-signed certificate use with an RSA cipher is output with the specified file name. The content of the self-signed certificate for use with Elliptic Curve Cryptography is output with the `ecc-` prefix at the beginning of the file name.

If you omit this option, files named `httpsd.txt` and `ecc-httpsd.txt` are output to the default output destination path.

/validity ***expiration-date-of-self-signed certificate***

Specify the expiration date of the self-signed certificate by using the number of days. The same values are applied for both the RSA cipher and Elliptic Curve Cryptography.

If you omit this option, the expiration date is 3,650 days. You can specify a value that is greater than or equal to the

number of days remaining until December 31, 9999.

/dname ***distinguished-name (DN)***

Specify the distinguished-name (DN) described in the SSL server certificate, in the format "attribute-type=attribute-value". The same values are applied for both the RSA cipher and Elliptic Curve Cryptography.

You can specify several attribute type values by using a comma (,) as a delimiter. Characters specified as the attribute type are not case sensitive. You cannot use a double quotation mark or a backslash in the attribute type.

For details about how to escape characters, follow the instructions in RFC 2253.

To escape the following symbols, use a backslash.

- Plus signs, commas, semicolons (;), left angle brackets (<), equal signs, right angle brackets (>)
- Spaces at the beginning of character strings
- Spaces at the end of character strings
- Hash marks at the beginning of character strings

If you omit this option, you need to enter attribute values according to the instructions on the window displayed when you execute the command.

The following table lists the attribute types that can be specified for this option:

Attribute type	Meaning of attribute type	Wording on window at response entry	Attribute value
CN	Common Name	Server Name	Distinguished-name# of the JP1/OA server, such as host name, IP address, or domain name
OU	Organizational Unit Name	Organizational Unit	Lower-level organization name, such as department or section name
O	Organization Name	Organization Name	Company or other organization's name#
L	Locality Name	City or Locality	City name or region name (city, town, or village name for Japan)
ST	State or Province Name	State or Province	State name or district name (prefecture name for Japan)
C	Country Name	two-character country-code	Country code (JP for Japan)

#: Required in a response entry

The following is an example of response input:

```
Enter Server Name [default=MyHostname]:example.com
Enter Organizational Unit:Device Manager Administration
Enter Organization Name [default=MyHostname]:HITACHI
Enter your City or Locality:Yokohama
Enter your State or Province:Kanagawa
Enter your two-character country-code:JP
Is CN=example.com,OU=Device Manager Administration,O=HITACHI,L=Yokohama, ST=Kanagawa,C=JP
```

```
correct? (y/n) [default=n]:y
```

If the entry is incorrect, enter n in order to re-enter the response.

/sigalg ***signature-algorithm-for-server-certificate-for-RSA-cipher***

Specify a signature algorithm for the server certificate for the RSA cipher. You can specify SHA1withRSA, SHA256withRSA, or SHA512withRSA.

If you omit this option, SHA256withRSA is used.

/eccsigalg ***signature-algorithm-for-server-certificate-for-elliptic-curve-cipher***

Specify a signature algorithm for the server certificate for the elliptic curve cipher. You can specify SHA1withECDSA, SHA256withECDSA, SHA384withECDSA, or SHA512withECDSA.

If you omit this option, SHA384withECDSA is used.

/ecckeysize ***keysize-of-private-key-for-elliptic-curve-cipher***

Specify the size of the private key for the elliptic curve cipher in bits. You can specify 256 or 384.

If you omit this option, the key size is 384 bits.

The size of a private key for an RSA cipher is 2,048 bits (fixed).

Storage location

installation-destination-folder-of-common-component`\bin`

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- If the attribute type CN of the SSL server certificate does not match the host name, IP address, or domain name specified as the connection destination of the JP1/OA server from the web browser, a warning or an error message is issued to indicate a server name mismatch.
- If this command is executed without specifying the `key`, `csr`, `cert`, or `certtext` option, each file is output to the following location:
  installation-destination-folder-of-common-component`\uCPSB\httpsd\conf\ssl\server`

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
249	The file or folder already exists on the specified path.

Return value	Description
250	Deletion of the key store failed.
251	Creation of the private key failed.
252	Creation of the self-signed certificate failed.
253	Creation of the CSR failed.
254	Creation of the content file of the self-signed certificate failed.
255	The command finished abnormally.

7.6.6 hcmds64checkcerts (checks the expiration date of the SSL server certificate)

Functionality

This command checks the expiration date of the following SSL server certificates that are specified in the `user_httpsd.conf` file, for when an HTTPS connection is used between JP1/OA and the Web browser.

- The SSL server certificate for common components (for RSA cipher and Elliptic Curve Cryptography)
- The SSL server certificate issued by chained certificate authorities

The SSL server certificate has an expiration date. Make sure that the certificate is not expired.

Format

hcmds64checkcerts

{[/days ***number-of-days***] [/log] | /all}

Arguments

/days ***number-of-days***

Specify the number of days to check whether the SSL server certificate is expired, counting from the day when the command was executed. The specifiable value range is from 30 to 3652 days (10 years). When this option is specified, SSL server certificates that will expire within the specified number of days and SSL server certificates that have already expired will be displayed.

If you omit this option, 30 is specified as the number of days.

/log

If the SSL server certificate to be displayed exists, a warning message will be displayed in the event log. To regularly check the expiration date of the SSL server certificate by registering this command in an OS task, specify this option.

/all

Displays the expiration date of all SSL server certificates specified in the user_httpsd.conf file.

Storage location

installation-destination-folder-of-common-component`\bin`

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	There are no SSL server certificates whose validity period expires within the number of days specified for the `days` option, and no SSL server certificates whose validity period has expired. If the `all` option is specified, the commend reports that it has ended normally regardless of whether any expiration dates have passed.
1	The argument is invalid.
253	The SSL server certificate to be checked does not exist.
254	There is more than one SSL server certificate whose validity period expires within the number of days specified in the `days` option, or whose validity period has already expired.
255	The command finished abnormally.

Example

The following example shows the use of this command to check the validity of an SSL server certificate:

- To confirm the existence of an SSL server certificate whose validity period expires within 60 days from the day the command is executed:
  hcmds64checkcerts /days 60
- To check the validity period of all SSL server certificates that are specified in the `user_httpsd.conf` file:
  hcmds64checkcerts /all

7.7 Operation-related commands

7.7.1 addconsumers (create consumers)

Functionality

This command creates a consumer by using a CSV file.

Format

addconsumers

/settingfile ***configuration-information-file***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/settingfile ***configuration-information-file***

Use an absolute or relative path to specify a CSV file that includes the configuration information of the consumer to be created. Save the file with UTF-8 encoding.

Input format

The following table shows the settings to be specified in the configuration information file. For details about the CSV file format, see *Appendix G. Format for Input/Output of Setting Information to CSV Files.*

Settings	Required	Value to be specified
ConsumerName	Y	The name of the consumer
Description	O	The description of the consumer
Grade	Y	A numerical value for the grade - 0: Platinum - 10: Gold - 20: Silver - 30: Bronze
URL	O	URL for the link
URLDisplayNames	O	Display name for the link

(Legend): Y: Required, O: Optional

Input example

```
#ConsumerName,Description,Grade,URL,URLDisplayNames
ConsumerName1,description1,0,URL1,URLDisplayNames1
ConsumerName2,description2,10, ,
ConsumerName3, ,20,URL3,URLDisplayNames3
ConsumerName4,description4,30,URL4,URLDisplayNames4
```

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
201	The input file format is invalid.
202	Consumer information with same name already exists.
203	You do not have permission to create this information.
222	Creating the consumer information failed.

Return value	Description
255	The command finished abnormally.

Example

The following example shows the use of this command to create configuration information for a consumer:

addconsumers /settingfile "C:\temp\SettingFile.csv" /user user01 /passwordfile PasswordFilePath

7.7.2 addsetting (creates configuration information)

Functionality

This command creates configuration information for the resources managed by JP1/OA.

Format

addsetting

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

/settingfile ***configuration-information-file***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

Specify the type of configuration information to be created.

- ipaddrrange: Specify this to add a search range of IP addresses in which the managed resources exist.
- credential: Specify this to add authentication information to be used for connecting to the managed resources.
- collector: Specify this to add a collector. Note that you cannot add a custom collector by using the `addsetting` command.
- userthresholdprofile: Specify this to add a threshold profile to be used for monitoring the managed user resources.
- systemthresholdprofile: Specify this to add a threshold profile to be used for monitoring the managed system resources.
- consumer: Specify this to create a consumer.

/settingfile ***configuration-information-file***

Specify the absolute or relative path of a JSON file that contains the configuration information to be created. The settings to be specified differ depending on the type of configuration information to be created. When specifying information in the JSON file, refer to the template file or default profile for the configuration information you want to create. For details about the files you can refer to, see *7.5 Overview of using commands to perform operations for JP1/OA configuration information*.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
201	The input file format is invalid.
202	A resource with the same name exists, or a duplicate search range exists.
203	You do not have permission to create this information.
207	Associating the authentication information specified for the search range failed.
219	Linkage with multiple JP1/IM instances is not possible.
222	Creating the information failed.

Return value	Description
255	The command finished abnormally.

Example

The following is an example of using the command to create configuration information for a search range:

addsetting /type ipaddrrange /settingfile "C:\temp\SettingFile.json" /user user01 /passwordfile PasswordFilePath

7.7.3 deletesetting (deletes configuration information)

Functionality

This command deletes the configuration information for the resources managed by JP1/OA.

Format

deletesetting

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

/name ***name-of-information-to-be-deleted***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

Specify the type of configuration information to be deleted.

- ipaddrrange: Specify this to delete a search range of IP addresses in which the managed resources exist.
- credential: Specify this to delete authentication information used for connecting to the managed resources.
- collector: Specify this to delete a collector. Note that you cannot delete a custom collector by using the `deletesetting` command.
- userthresholdprofile: Specify this to delete a threshold profile used for monitoring the managed user resources.
- systemthresholdprofile: Specify this to delete a threshold profile used for monitoring the managed system resources.
- consumer: Specify this to delete a consumer.

/name ***name-of-information-to-be-deleted***

Specify the name of the configuration information to be deleted.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks,

backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1*/OA*\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
201	The specified collector connot be deleted.
208	The specified authentication information cannot be deleted because it is being used.
209	The default threshold profile cannot be deleted.
212	You do not have permission to delete this information.
222	An attempt to delete the information failed.
224	The information does not exist.
255	The command finished abnormally.

Example

The following is an example of using the command to delete the configuration information for a search range:

deletesetting /type ipaddrrange /name range01 /user user01 /passwordfile PasswordFilePath

7.7.4 disablemonitoring (stops monitoring)

Functionality

This command invalidates the monitoring status of a resource managed by JP1/OA.

Format

disablemonitoring

/id ***resource-ID***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***resource-ID***

Specify the ID of the resource for which you change the monitoring status. You can use the listresources command to check the resource ID.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- Execution of the command requires that the JP1/OA service is activated.
- You can invalidate only the resources being managed by JP1/OA by executing the disablemonitoring command.

Resources to be excluded and deleted resources are not subject to the command processing.

- Specify a user that has the Admin or Modify permission as the user of JP1/OA that you specify when executing the command.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
223	Invalidation of the monitoring status failed.
224	The specified resource does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to invalidate the monitoring status:

disablemonitoring /id hv1 /user user01 /passwordfile PasswordFilePath

7.7.5 enablemonitoring (executes monitoring)

Functionality

This command validates the monitoring status of a resource managed by JP1/OA.

Format

enablemonitoring

/id ***resource-ID***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***resource-ID***

Specify the ID of the resource for which you change the monitoring status. You can use the listresources command to check the resource ID.

/user ***user-name***

Specify a user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1*/OA*\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- Execution of the command requires that the JP1/OA service is activated.
- You can validate only the resources being managed by JP1/OA by executing the enablemonitoring command. Resources to be excluded and deleted resources are not subject to the command processing.
- Specify a user that has the Admin or Modify permission as the user of JP1/OA that you specify when executing the command.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.

Return value	Description
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
222	Validation of the monitoring status failed.
224	The specified resource does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to validate the monitoring status:

enablemonitoring /id hv1 /user user01 /passwordfile PasswordFilePath

7.7.6 getsettings (obtains configuration information)

Functionality

This command obtains configuration information for the resources managed by JP1/OA.

Format

getsettings

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

/outputdir ***output-destination-folder***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

Specify the type of configuration information to be obtained.

- ipaddrrange: Specify this to obtain a search range of IP addresses in which the managed resources exist.
- credential: Specify this to obtain authentication information used for connecting to the managed resources.
- collector: Specify this to obtain a collector.
- userthresholdprofile: Specify this to obtain a threshold profile used for monitoring the managed user resources.
- systemthresholdprofile: Specify this to obtain a threshold profile used for monitoring the managed system resources.
- consumer: Specify this to obtain a consumer.

/outputdir ***output-destination-folder***

Use an absolute or relative path to specify a folder to which the obtained configuration information is to be output.

Configuration information is output for each instance ID.

For details about the format of the output file, refer to the template file or default profile for the configuration information you want to output.

For details about the files you can refer to, see *7.5 Overview of using commands to perform operations for JP1/OA*

configuration information.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
204	You do not have permission to view this information.

Return value	Description
222	An attempt to view the information failed.
224	The information does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to obtain a search range:

getsettings /type ipaddrrange /outputdir "C:\Output" /user user01 /passwordfile PasswordFilePath

7.7.7 hcmds64srv (starts, stops, or displays status of JP1/OA)

Functionality

This command starts or stops JP1/OA services and databases. The command also displays the JP1/OA service status or changes the service start method.

By executing this command by specifying AnalyticsWebService in the server option, you can start, stop, or display the status of the following services:

Service display name and process	Start	Stop	Status display
HAnalytics Engine Web Service	Y	Y	Y
HBase 64 Storage Mgmt Web Service	Y	N	N
HBase 64 Storage Mgmt Web SSO Service	Y	N	N
HAnalytics Engine	Y	Y	N
HAnalytics Engine Database _OA0	Y	Y	N
Database process#	Y	N	N

(Legend)

Y: Processed N: Not processed

#: Internal process of JP1/OA. The hcmds64srv command does not start or stop "HiRDB/EmbeddedEdition _HD1" which indicates a database service.

If you omit the server option, the next service is started, stopped, or the status of the next service is displayed. Also, if you omit the server option, you can use the statusall option which displays the status of all services.

Service display name and process	Start	Stop	Status display	Status display (/statusall)
HAnalytics Engine Web Service	Y	Y	Y	Y
HBase 64 Storage Mgmt SSO Service	Y	Y	Y	Y
HBase 64 Storage Mgmt Web Service	Y	Y	Y	Y
HBase 64 Storage Mgmt Web SSO Service	Y	Y	Y	Y
HAnalytics Engine	Y	Y	N	Y#1

Service display name and process	Start	Stop	Status display	Status display (/statusall)
HAnalytics Engine Database _OA0	Y	Y	N	Y[#1]
Database process[#2]	Y	Y	Y	Y
Service of products that use the common component	Y	Y	Y	Y

(Legend)

Y: Processed N: Not processed

#1: The statuses of "HAnalytics Engine" and "HAnalytics Engine Database _OA0" are displayed as "HAnalytics Engine". If either "HAnalytics Engine" or "HAnalytics Engine Database _OA0" is started, the service is judged as being started. If both "HAnalytics Engine" and "HAnalytics Engine Database _OA0" are stopped, the service is judged as being stopped.

#2: Internal process of JP1/OA. The hcmds64srv command does not start or stop "HiRDB/EmbeddedEdition _HD1" which indicates a database service.

Format

hcmds64srv

{/start | /stop | /check | /status}

[/server ***service-name***]

To check the status of services of JP1/OA and products that use the common component:

hcmds64srv

/statusall

To change the start method of a service:

hcmds64srv

/starttype {auto | manual}

{/server ***service-name*** | /all}

Arguments

/start

Starts the service and database you specified in the server option.

/stop

Stops the service and database you specified in the server option.

/check

Displays the status of the server and database you specified in the server option.

/status

Displays the status of the server and database you specified in the server option.

/server ***service-name***

To start, stop, or display the status of JP1/OA product services only, specify AnalyticsWebService as the service name. If you omit this option, the services of JP1/OA, and all products that use the common component, are subject to the command processing.

/statusall

Displays the service and data statuses, and the status of the products registered in the common component.

/starttype {auto | manual}

Specify the start type of the service specified with the server option.

Specify auto for an automatic start, and manual for a manual start.

/all

If you specify this option, all services of JP1/OA and other products that use common components are subject to the command processing. All JP1/OA services, and services of all products that use the common component, are subject to the command processing.

Storage location

installation-destination-folder-of-common-component\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- If you start or stop JP1/OA services as a daily operation, omit the server option to start or stop all the services. To start only JP1/OA services by specifying the "server" option, specify "AnalyticsWebService" for the "server" option to start the common component service.
- If you execute the command with the stop option specified and the termination processing does not end within three minutes, an error occurs and a message is displayed to indicate a time-out. In this case, wait a while, and then re-execute the command with the stop option specified.
- If you start or stop a service with the start/stop option specified, the command might end while the service does not start or stop completely. To confirm that the service has completely started or stopped, use either of the following operations:
  - Confirm that either of the following messages has been output to a disclosed log or the event log:
    Start: KNAQ10086-I Application is running.
    Stop: KNAQ10089-I Application is stopped.

- Specify the statusall option to check the status of the service.

Return values

The following table describes the return values of the command when the start option or stop option is specified:

Return value	Description
0	The command finished normally.
1	The service has already been started (when the start option is specified). The service has already been stopped (when the stop option is specified).
255	Execution of the command failed.

The following table describes the return values of the command when the check, status, or statusall option is specified:

Return value	Description
0	The service has not started yet.
1	The service has started.
255	Execution of the command failed.

The following table describes the return values of the command when the starttype option is specified:

Return value	Description
0	The command finished normally.
255	Execution of the command failed.

Example

The following examples show the use of this command to start, stop, or check the status of a service of a JP1/OA product:

- To start a service of a JP1/OA product:

  hcmds64srv /start /server AnalyticsWebService

- To stop a service of a JP1/OA product:

  hcmds64srv /stop /server AnalyticsWebService

- To check the status of a service of a JP1/OA product:

  hcmds64srv /status /server AnalyticsWebService

7.7.8 hcmds64unlockaccount (unlocks a user account)

Functionality

This command unlocks a user account. Use this command when you cannot log in to JP1/OA because all the user accounts are locked.

Format

hcmds64unlockaccount

/user ***user-ID***

/pass ***password***

Arguments

/user ***user-ID***

Specify the user ID of the user account to be unlocked. The user ID you specify must have the User Management permission.

/pass ***password***

Specify the password of the user account to be unlocked.

Storage location

installation-destination-folder-of-common-component\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- You can use the hcmds64unlockaccount command to unlock only user accounts that have the User Management permission.
- If the user name or password you specify in an option contains an ampersand, vertical bar, or caret, enclose each of these symbols with double quotation marks or add a caret before each symbol as an escape character. For example, if the password is ^a^b^c^ in Windows, use either hcmds64unlockaccount /user system /pass "^"a"^"b"^"c"^" or hcmds64unlockaccount /user system /pass ^^a^^b^^c^^.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
251	An authentication error (login error) occurred.
252	An authentication error (no User Management permission) occurred.
253	Communication with the authentication server failed.
254	The command was executed on the secondary server side.
255	The command finished abnormally.

Example

The following example shows the use of this command to unlock a user account:

hcmds64unlockaccount /user test01 /pass TTdate00

7.7.9 hcmds64chgurl (changes the URL of JP1/OA)

Functionality

This command changes the URL for accessing the JP1/OA server when the settings such as the host name, IP address, and port number for JP1/OA server are changed.

Format

hcmds64chgurl

{/list | /change ***URL-before-change URL-after-change*** | /change ***URL-after-change*** /type Analytics}

Arguments

/list

This option causes the command to display the list of URLs and product names currently set up.

/change ***URL-before-change URL-after-change***

This option causes the command to overwrite the URL related information currently registered with the new URL related information.

You specify both the URL that is currently registered and the new URL. If you use the option together with the type option, you only specify the new URL.

/type Analytics

This option specifies “Analytics” as the name of the product whose URL is to be changed.

Storage location

installation-destination-folder-of-common-component\bin

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	The URL cannot be found.
255	The command finished abnormally.

Example

The following examples show how to use the command for each case.

- To display the list of URLs and product names currently set up:
  hcmds64chgurl /list
- To overwrite the URL related information currently registered with the new URL related information:
  hcmds64chgurl /change "http://192.168.11.33:22015" "http://192.168.11.55:22015"

7.7.10 listconsumers (obtains the list of consumers)

Functionality

This command outputs the list of consumers to a CSV file.

Format

listconsumers

/outfile ***output-file***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/outfile ***output-file***

Use an absolute or relative path to specify a CSV file to which the list of consumers is to be output.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
204	You do not have permission to view this information.
222	Failed to obtain the consumer information.
255	The command finished abnormally.

Example

The following example shows the use of this command to obtain a list of consumers:

```
listconsumers /outfile "C:\temp\outfile.csv" /user user01 /passwordfile PasswordFilePath
```

Output format

The following table shows the content of the output file. For details about the CSV file format, see *Appendix G. Format for Input/Output of Setting Information to CSV Files.*

Settings	Value to be specified
ConsumerName	The name of the consumer
Description#	The description of the consumer
Grade	A numerical value for the grade - 0: Platinum - 10: Gold - 20: Silver - 30: Bronze

Settings	Value to be specified
URL[#]	URL for the link
URLDisplayNames[#]	Display name for the link

#: If this is not set, nothing is output.

Output example

```
#JP1/Operations Analytics,111000,UTF-8 (BOM)
#Consumer Information
#2016-12-26T12:47:30.421+0900
#ConsumerName,Description,Grade,URL,URLDisplayNames
ConsumerName1,description1,0,URL1,URLDisplayNames1
ConsumerName2,description2,10,,
ConsumerName3, ,20,URL3,URLDisplayNames3
ConsumerName4,description4,30,URL4,URLDisplayNames4
```

7.7.11 listresources (lists resource information)

Functionality

This command lists resource information managed by JP1/OA, in CSV format.

Format

listresources

/type {hypervisor | vm | storagesystem | volume | ipswitch | fcswitch | host | application}

/user ***user-name*** /passwordfile ***password-file***

Arguments

/type {hypervisor | vm | storagesystem | volume | ipswitch | fcswitch | host | application}

Specify one of the following as the type of resource to be output:

- hypervisor

  Outputs a Hypervisor list.

- vm

  Outputs a VirtualMachine list.

- storagesystem

  Outputs a StorageSystem list.

- volume

  Outputs a Volume list.

- ipswitch

  Outputs an IPSwitch list.

- fcswitch

  Outputs an FCSwitch list.

- host

  Outputs a Host list.

- application

  Outputs an Application list.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- Execution of the command requires that the JP1/OA service is activated.
- You can output a list of information only for the resources being managed by of JP1/OA by executing the listresources command. Resources to be excluded and deleted resources are not subject to the command processing.
- Specify a user that has the Admin or Modify permission as the user of JP1/OA that you specify when executing the command.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.

Return value	Description
3	The service status of JP1/OA is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
221	Acquisition of a resource list failed.
255	The command finished abnormally.

Example

The following example shows the use of this command to output a Hypervisor list:

listresources /type hypervisor /user user01 /passwordfile PasswordFilePath

Output example

The following is an example of outputting a Hypervisor list:

"ID","Hypervisor Name","IP Address","Monitoring","Cluster Name","Access Point"
"hv3","12.34.56.103","12.34.56.103","Enabled","","Type:vCenter,IP Address/Host Name:12.34.56.10, User ID:Administrator, Collector Name:12.34.56.10"
"hv2","12.34.56.102","12.34.56.102","Enabled","Cluster","Type:vCenter,IP Address/Host Name:12.34.56.10, User ID:Administrator, Collector Name:12.34.56.10"
"hv1","12.34.56.101","12.34.56.101","Enabled","","Type:vCenter,IP Address/Host Name:12.34.56.10, User ID:Administrator, Collector Name:12.34.56.10"

7.7.12 outputevent (outputs event information to a CSV file)

Functionality

This command outputs to a CSV file the event information managed by JP1/OA.

Format

outputevent

[/id ***resource-ID***]

/from ***start-time*** [{/to ***end-time***| /timeperiod ***period-for-which-event-information-is-obtained***}]

/outputpath ***output-CSV-file-path***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***resource-ID***

Specify the resource ID to output relevant event information. The resource ID can be checked by using the `listresources` command. If this option is omitted, all event information will be output.

The specifiable resource ID types are as follows:

- hypervisor
- storage system
- ip switch
- fc switch
- host

/from ***start-time***

Specify the start time from which event information is obtained.

Specify the time in *yyyymmddhhmm* format.

If the `to` option or the `timeperiod` option is omitted, the default period for which information will be obtained is 24 hours (`24h`) is used.

/to ***end-time***

Specify the end time to which event information is obtained.

Specify the time in *yyyymmddhhmm* format.

This option cannot be specified together with the `timeperiod` option.

/timeperiod ***period-for-which-event-information-is-obtained***

Specify the period for which event information is obtained.

Specify the period in the following format:

- `1h` to `48h` (Append `h` to a numerical value from 1 to 48): This means that the period is from 1 hour to 48 hours from the start time.
- `1d` to `120d` (Append `d` to a numerical value from 1 to 120): This means that the period is from 1 day to 120 days from the start time.

This option cannot be specified together with the `to` option.

/outputpath ***output-CSV-file-path***

Specify the path of the CSV file to be output, as either an absolute or a relative path.

If a file with the same name exists in the output destination, delete that file or move it to a different location. For details about the format of the output file, see *Appendix F. Format for Output of Resource Information to CSV Files*.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:
Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

/passwordfile ***password-file***
Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location
installation-destination-folder-of-JP1/OA\bin

Execution permissions
The Administrator permission is required to perform this operation.

Notes
- Execution of the command requires that the JP1/OA service is activated.
- If a large number of events are to be output, it might take an hour or longer to create a CSV file containing the event information, and the information might not be output normally. When this occurs, limit the number of events to be output by using the options "/from" and "/to" or the option "/timeperiod" to specify the period for which event information is output, and then execute the command.

Return values
The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
210	Creating a CSV file failed.
224	The specified resource does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to output all event information from 9:00 to 21:00 on December 1, 2016, to a CSV file:

outputevent /from 201612010900 /to 201612012100 /outputpath "C:\Output\event01.csv" /user user01 /passwordfile PasswordFilePath

7.7.13 outputlatestperf (outputs performance information (the most recent values) to a CSV file)

Functionality

This command outputs to a CSV file the performance information (the most recent values) for the resources managed by JP1/OA.

Format

outputlatestperf

/id ***resource-ID***

/outputpath ***output-CSV-file-path***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***resource-ID***

Specify the resource ID for which performance information will be output. The resource ID can be checked by using the `listresources` command.

The specifiable resource ID types are as follows:

- hypervisor
- vm
- volume
- ip switch
- fc switch
- host
- cpu
- memory
- hba
- nic
- disk

/outputpath ***output-CSV-file-path***

Specify the path of the CSV file to be output, as either an absolute or a relative path.

If a file with the same name exists in the output destination, delete that file or move it to a different location. For details about the format of the output file, see *Appendix F. Format for Output of Resource Information to CSV Files*.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
210	Creating a CSV file failed.

Return value	Description
224	The specified resource does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to output the performance information (the most recent values) for a virtual machine, "vm777", to a CSV file:

outputlatestperf /id vm777 /outputpath "C:\Output\vm777latest.csv" /user user01 /passwordfile PasswordFilePath

7.7.14 outputresource (outputs resource information to a CSV file)

Functionality

This command outputs to a CSV file resource information or a list of related resources managed by JP1/OA.

Format

outputresource

/id ***resource-ID*** [/withrelation]

/outputpath ***output-CSV-file-path***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***resource-ID*** [/withrelation]

Specify the resource ID for which resource information is output. The resource ID can be checked by using the `listresources` command.

The specifiable resource ID types are as follows:

- hypervisor
- vm
- storage system
- volume
- ip switch
- fc switch
- host
- application
- cpu
- memory
- hba
- nic
- disk
- consumer[#]

- cluster#

#:
You cannot specify the resource ID when the `withrelation` option is specified.

/withrelation
Specify this option if you want to output the list of resources that are related to the resource ID specified by the `ID` option.

/outputpath ***output-CSV-file-path***
Specify the path of the CSV file to be output, as either an absolute or a relative path.
If a file with the same name exists in the output destination, delete that file or move it to a different location. For details about the format of the output file, see *Appendix F. Format for Output of Resource Information to CSV Files*.

/user ***user-name***
Specify the user name of the JP1/OA user for whom the command will be executed.
You can specify from 1 to 256 characters.
You can use alphanumeric characters and the following characters:
Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

/passwordfile ***password-file***
Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location
installation-destination-folder-of-JP1/OA`\bin`

Execution permissions
The Administrator permission is required to perform this operation.

Notes
Execution of the command requires that the JP1/OA service is activated.

Return values
The following table describes the return values of the command:

Return value	Description
0	The command finished normally.

Return value	Description
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
210	Creating a CSV file failed.
224	The specified resource does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to output the resource information for a virtual machine, "vm777", to a CSV file:

outputresource /id vm777 /outputpath "C:\Output\vm777info.csv" /user user01 /passwordfile PasswordFilePath

7.7.15 outputtimeseriesperf (outputs performance information (in chronological order) to a CSV file)

Functionality

This command outputs to a CSV file performance information (in chronological order) for the resources managed by JP1/OA.

Format

outputtimeseriesperf

/id ***performance-ID***

/from ***start-time*** [{/to ***end-time***| /timeperiod ***period-for-which-performance-information-is-obtained***}]

/outputpath ***output-CSV-file-path***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/id ***performance-ID***

Specify the performance ID of the performance information that is to be output. You can specify a maximum of 10 IDs). To specify multiple IDs, use commas (,) to separate each ID.

The performance ID to be specified can be checked by using the `outputlatestperf` command.

/from ***start-time***

Specify the start time from which performance information is obtained.

Specify the time in *yyyymmddhhmm* format.

If the `to` option or the `timeperiod` option is omitted, the default period for which information will be obtained is 24 hours (`24h`) is used.

/to ***end-time***

Specify the end time to which performance information is obtained.

Specify the time in *yyyymmddhhmm* format.

This option cannot be specified together with the `timeperiod` option.

/timeperiod ***period-for-which-event-information-is-obtained***

Specify the period for which performance information is obtained.

Specify the period in the following format:

- `1h` to `48h`: Append `h` to a numerical value from 1 to 48. This means that the period is from 1 hour to 48 hours from the start time.
- `1d` to `120d`: Append `d` to a numerical value from 1 to 120. This means that the period is from 1 day to 120 days from the start time.

This option cannot be specified together with the `to` option.

/outputpath ***output-CSV-file-path***

Specify the path of the CSV file to be output, as either an absolute or a relative path.

If a file with the same name exists in the output destination, delete that file or move it to a different location. For details about the format of the output file, see *Appendix F. Format for Output of Resource Information to CSV Files*.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

***installation-destination-folder-of-JP1/OA*\bin**

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
8	The specified path already exists.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
210	Creating a CSV file failed.
225	The specified performance ID does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to output performance information for IDs 1 and 2 during the 24 hour period starting from 00:00 on December 1, 2016, to a CSV file:

outputtimeseriesperf /id 1,2 /from 201612010000 /outputpath "C:\Output\series.csv" /user user01 /passwordfile PasswordFilePath

7.7.16 reloadproperty (re-reads a definition file)

Functionality

Reloads the following definition file.

- Definition files for linking with JP1/SS or JP1/NP.
- Definition files for setting up templates for the commands to be executed in the Execute Action window.
- Definition files for mapping between applications and hosts.

- Collector definition files for monitoring applications.

The following table describes the type of the definition file that the command references, and the reference destination folder:

Type of definition file	Reference destination folder in a non-cluster system	Reference destination folder in a cluster system
Definition file for linking with JP1/SS or JP1/NP	***installation-destination-folder-of-JP1/OA***\conf\template\mail	***shared-folder-name***\Analytics\conf\template\mail
Definition files for setting up templates for the commands to be executed in the Execute Action window	***installation-destination-folder-of-JP1/OA***\conf\template\command	***shared-folder-name***\Analytics\conf\template\command
Definition files for mapping between applications and hosts (when linked with JP1 products)	***installation-destination-folder-of-JP1/OA***\conf	***shared-folder-name***\Analytics\conf
Definition files for mapping between applications and hosts (when a custom collector is registered)	***installation-destination-folder-of-JP1/OA***\lib\collector\application***collector-folder***\conf	***shared-folder-name***\Analytics\lib\collector\application***collector-folder***\conf
Collector definition files for monitoring applications (when a custom collector is registered)	***installation-destination-folder-of-JP1/OA***\lib\collector\application***collector-folder***	***shared-folder-name***\Analytics\lib\collector\application***collector-folder***

Format

reloadproperty

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
3	The service status is invalid.
5	Communication failed.
14	You do not have permission to execute this command.
231	The re-reading of the definition file failed.
255	The command finished abnormally.

7.7.17 updatecredentials (edits authentication information)

Functionality

This command uses a CSV file to edit the authentication information used to access resources managed by JP1/OA.

Format

updatecredentials

/type {WMI | SSH | SNMP | SNMPv3 | WBEM | IM | AJS | PFM | vCenter}

/settingfile ***configuration-information-file***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/type {WMI | SSH | SNMP | SNMPv3 | WBEM | IM | AJS | PFM | vCenter }

Specify the type of the protocol or collector whose authentication information you want to edit.

- WMI: Windows, Windows Hyper-V
- SSH: Linux, HP-UX, AIX, Solaris
- SNMP: Switch for which the SNMP version is v1 or v2c (IP switch or FC switch).
- SNMPv3: Switch for which the SNMP version is v3 (IP switch or FC switch).
- WBEM: FC switch, storage system
- IM: JP1/IM - Manager
- AJS: JP1/AJS3 - Manager
- PFM: JP1/PFM - Manager
- vCenter: vCenter

/settingfile ***configuration-information-file***

Specify the absolute or relative path of a CSV file that contains configuration information. Save the file with UTF-8 encoding.

The settings to be specified differ depending on the type of authentication information to be edited.

For details about the CSV file format, see *Appendix G. Format for Input/Output of Setting Information to CSV Files.*

For WMI

Settings	Required	*Value to be specified*
CredentialName	Y	*Name of the authentication information*
CredentialUserId	Y	*User ID of the authentication information*
CredentialPassword	Y	*Password of the authentication information*

(Legend): Y: Required

An example configuration information file (for WMI)

```
#Credentialname,CredentialUserId,CredentialPassword
Credentialname1,CredentialUserId1,CredentialPassword1
Credentialname2,CredentialUserId2,CredentialPassword2
```

For SSH

Settings	Required	Value to be specified
CredentialName	Y	Name of the authentication information
CredentialUserId	Y	User ID of the authentication information
CredentialPassword	Y	Password of the authentication information
rootpassword	Y	Administrator password

(Legend): Y: Required

An example configuration information file (for SSH)

```
#Credentialname,CredentialUserId,CredentialPassword,rootPassword
Credentialname1,CredentialUserId1,CredentialPassword1,rootPassword1
Credentialname2,CredentialUserId2,CredentialPassword2,rootPassword2
```

For SNMP

Settings	Required	Value to be specified
CredentialName	Y	Name of the authentication information
CommunityName	Y	Community name of the authentication information

(Legend): Y: Required

An example configuration information file (for SNMP)

```
#Credentialname,CommunityName
Credentialname1,CommunityName1
Credentialname2,CommunityName2
```

For SNMPv3

Settings	Required	Value to be specified
Credentialname	Y	Name of the authentication information
userName	Y	User name
authenticationEnabled	Y	- `true`: Enables authentication. - `false`: Disables authentication.
authenticationPassphrase	Y[#1]	Passphrase for authentication
authenticationProtocol	Y[#1]	- `MD5`: Use MD5 - `SHA`: Use SHA
privacyEnabled	Y	- `true`: Enables privacy. - `false`: Disables privacy.
privacyPassphrase	Y[#2]	The passphrase for privacy
privacyProtocol	Y[#2]	- `AES128`: Use AES128 - `DES`: Use DES

(Legend): Y: Required

#1: If you specify `true` for `authenticationEnabled`, you must specify a value for this setting.

#2: If you specify `true` for `privacyEnabled`, you must specify a value for this setting.

An example configuration information file (for SNMPv3)

```
#Credentialname,UserName,authenticationEnabled,authenticationPassphrase,
#authenticationProtocol,privacyEnabled,privacyPassphrase,privacyProtocol
Credentialname1,UserName1,true,authenticationPassphrase1,MD5,true,privacyPassphrase1,AES128
Credentialname2,UserName2,true,authenticationPassphrase2,SHA,false,,,
Credentialname3,UserName3,false,,,true,privacyPassphrase2,DES
Credentialname4,UserName4,false,,,false,,,
```

For WBEM

Settings	Required	Value to be specified
CredentialName	Y	Name of the authentication information
UserId	Y	User ID
Password	Y	Password used to access the resource

(Legend): Y: Required

An example configuration information file (for WBEM)

```
#CredentialName,UserId,Password
CredentialName1,UserID1,Password1
CredentialName2,UserID2,Password2
CredentialName3,UserID3,Password3
```

For collector

Settings	Required	Value to be specified
CollectorName	Y	Name of the collector
UserId	Y	User ID
Password	Y	Password
RootPassword	Y#	Administrator password

(Legend): Y: Required

#: This setting is not required if the OS type of the collector is Windows.

An example configuration information file (for collector)

```
#CollectorName,UserId,Password,RootPassword
CollectorName1,UserId1,Password1,RootPassword1
CollectorName2,UserId2,Password2,RootPassword2
CollectorName3,UserId3,Password3,RootPassword3
```

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
201	The input file format is invalid.
202	Authentication information with the same name exists.
204	You do not have permission to view this information.
205	You do not have permission to update this information.
222	Editing the information failed.
224	The information does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to edit the SSH authentication information:

updatecredentials /type SSH /settingfile C:\temp\SettingFile.csv /user user01 /passwordfile PasswordFilePath

7.7.18 updatesetting (edits configuration information)

Functionality

This command edits configuration information for JP1/OA.

Format

updatesetting

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

/settingfile ***configuration-information-file***

/user ***user-name***

/passwordfile ***password-file***

Arguments

/type {ipaddrrange | credential | collector | userthresholdprofile | systemthresholdprofile | consumer}

Specify the type of configuration information to be edited.

- ipaddrrange: Specify this to edit a search range of IP addresses in which the managed resources exist.
- credential: Specify this to edit authentication information used for connecting to the managed resources.

- collector: Specify this to edit a collector. Note that you cannot edit a customer collector by using the `updatesetting` command.
- userthresholdprofile: Specify this to edit a threshold profile used for monitoring the managed user resources.
- systemthresholdprofile: Specify this to edit a threshold profile used for monitoring the managed system resources.
- consumer: Specify this to edit a consumer.

/settingfile ***configuration-information-file***

Use an absolute or relative path to specify the JSON file that includes the configuration information to be edited. The settings to be specified differ depending on the type of configuration information to be edited. When writing information in the JSON file, refer to the template file or default profile for the configuration information you want to edit.

For details about the files you can refer to, see *7.5 Overview of using commands to perform operations for JP1/OA configuration information*.

/user ***user-name***

Specify the user name of the JP1/OA user for whom the command will be executed.

You can specify from 1 to 256 characters.

You can use alphanumeric characters and the following characters:

Exclamation marks (!), hash marks, dollar signs ($), percent signs (%), ampersands (&), single quotation marks ('), left parentheses, right parentheses, asterisks (*), plus signs (+), hyphens, periods, equal signs (=), at marks, backslashes, carets (^), underscores, and vertical bars (|)

The user name is not case sensitive.

/passwordfile ***password-file***

Specify the path of the file in which the password of the user specified in the user option is stored, in absolute or relative path format.

Storage location

installation-destination-folder-of-JP1/OA`\bin`

Execution permissions

The Administrator permission is required to perform this operation.

Notes

Execution of the command requires that the JP1/OA service is activated.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
5	Communication failed.
6	An authentication error occurred.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
201	The input file format is invalid.
202	A resource with the same name exists, or a duplicate search range exists.
204	You do not have permission to view this information.
205	You do not have permission to update this information.
206	The authentication information record with the specified name does not exist.
207	Associating the authentication information specified for the search range failed.
222	Editing the information failed.
224	The information does not exist.
255	The command finished abnormally.

Example

The following example shows the use of this command to edit configuration information for a search range:

```
updatesetting /type ipaddrrange /settingfile "C:\temp/SettingFile.json" /user user01 /passwordfile
PasswordFilePath
```

7.8 Maintenance-related commands

7.8.1 backupsystem (backs up the JP1/OA system)

Functionality

This command backs up JP1/OA configuration information or database information in the folder you specify.

Format

backupsystem

/dir ***output-directory***

/type {all | Analytics}

[/auto]

Arguments

/dir ***output-directory***

Specify an empty folder for collecting backup data in absolute or relative path format.

/type {all | Analytics}

Specify the backup target.

- all

  Backs up information in JP1/OA and the common component.

  Manages user information in the common component.

- Analytics

  Backs up information of JP1/OA only.

/auto

Automatically stops or starts services and databases of JP1/OA and products that use the common component. If you omit this option, these services and databases are not stopped or started automatically.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- Make sure that the folder in which the backup file is to be stored has a sufficient amount of free space. The following is the amount of required free space:

  For non-cluster systems:

  Capacity of folders and files under ***installation-directory-of-JP1/OA***\data\database + 5

GB

For cluster systems:

Capacity of folders and files under ***shared-folder-name***\Analytics\data\database + 5 GB

If products that use the common component are included, add the capacity required for backing up information for these products in the calculation.

- The files below are not backed up. If necessary, back up these files manually.
  - SSL server certificate file for https connections
  - Private-key file for https connections

  The files for https connections are defined in the httpsd.conf file and the user_httpsd.conf file.
- If all of the following conditions are met, use the hcmds64srv command to stop the service before executing the backupsystem command:
  - The auto option is specified.
  - All was specified in the type option.
- In an environment where JP1/OA coexists with JP1/AO and products that use the common component, execute the restoresystem command by specifying "/type Analytics" to restore only JP1/OA data. You can acquire the backup files required for restoration above by specifying "/type Analytics".

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
4	Another command is currently executing.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
11	The specified folder is not empty.
14	You do not have permission to execute this command.
100	The backup operation failed.
101	The start or stop of the service failed.
255	Command execution was interrupted due to an error other than above.

Example

The following example shows the use of this command to back up information of JP1/OA only:

```
backupsystem /dir "C:\Users\Backup" /type Analytics /auto
```

7.8.2 expandretention (extends the retention period for performance information)

Functionality

This command extends the retention period for performance information retained by JP1/OA if you specified a value other than the default value for the retention period for performance information at the time of installation.

Format

expandretention

{/perf 1 | 2 | 3 | 4 /dir ***temporary-directory*** [/auto]

| /check}

Arguments

/perf {1 | 2 | 3 | 4}

Specify one of the following values (number of months) for performance information to be retained. You cannot make changes to shorten the period.

- 1

Extend the retention period to 1 month.

- 2

Extend the retention period to 2 months.

- 3

Extend the retention period to 3 months.

- 4

Extend the retention period to 4 months.

/dir ***temporary-directory***

Specify the temporary folder when the retention period is changed, in absolute or relative path format.

/auto

Automatically stop or start the services and databases for the products that use JP1/OA and common components. If you omit this option, the services and databases of the products that use JP1/OA and common component will not be automatically stopped or started.

/check

Specify to display the current retention period.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

According to the current retention period settings, free capacity is required as follows for the temporary directory that is specified when the `expandretention` command is executed:

- If the retention period before the extension is 14 days: 20 GB
- If the retention period before the extension is 1 month: 50 GB
- If the retention period before the extension is 2 months: 50 GB
- If the retention period before the extension is 3 months: 110 GB
- If the retention period before the extension is 4 months: 140 GB

Return values

The following table describes return values for the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
4	Another command is currently executing.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
11	The specified folder is not empty.
14	You do not have permission to execute this command.
101	The start or stop of the service failed.
242	The same retention period as the current setting was specified.
243	A retention period shorter than the current setting was specified.
245	Executing the command to extend the retention period failed.
255	Command execution was interrupted due to an error other than above.

Example

The following examples show the use of this command to extend or display the retention period:

- To extend the retention period to 2 month:

  expandretention /perf 2 /dir "C:\tempfolder" /auto

- To display the current retention period:

  expandretention /check

7.8.3 hcmds64getlogs (collects log information)

Functionality

This command collects log information that is output during operation of JP1/OA, and then outputs the log

information to an archive file.

Format

hcmds64getlogs

/dir ***output-folder-path***

[/types Analytics]

[/arc ***archive-file-name***]

[/logtypes {log | db | csv}]

Arguments

/dir ***output-folder-path***

Specify the folder path for outputting the archive file. You can specify only a folder of a local disk.

As the output folder path, specify an empty folder in absolute or relative path format. If the specified folder does not exist, the folder will be created.

The maximum allowable path length is 100 characters. The Write permission is set for the folder you specify in this option.

/types Analytics

Specify Analytics as the product name of the target of log information collection. This is not case sensitive. If you omit this option, JP1/OA and all Hitachi Command Suite products that have been installed are subject to the command processing. In this case, log collection might take a long time.

/arc ***archive-file-name***

Specify the name of the archive file to be created as the result of the common component's material collection tool. If you omit this option, the archive file name is HiCommand_log.

Archive files are output under the folder specified in the dir option.

Characters that can be specified as the archive file name include printable ASCII characters (0x20 to 0x7E), excluding the following special characters:

Backslashes, slashes (/), colons, commas, semicolons, asterisks, question marks, double quotation marks, left angle brackets, right angle brackets, vertical bars, dollar signs, percent signs, ampersands, single quotation marks, and grave accent marks (`)

You do not need to specify an extension.

/logtypes {log | db | csv}

Specify the type of the log file for the common component for which you want to collect logs. The following table shows the correspondence between the log file type and the log files that can be acquired:

Log file type	Log file that can be acquired
log	- Archive file name specified in the arc option_64.jar - Archive file name specified in the arc option.hdb_64.jar

Log file type	Log file that can be acquired
db	Archive file name specified in the arc option.db_64.jar
csv	Archive file name specified in the arc option.csv_64.jar

If you omit this option, all log files of the common component are acquired. Therefore, we recommend that you execute the command by omitting the option.

To specify more than one log file type, use a space as a delimiter (for example, "/logtypes log db csv"). If you use the types option and the logtypes option at the same time, specify "log" as the value of the logtypes option.

Output format

The following table lists the data collected as a result of the command execution:

In the case of cluster environment, a part of the information of mention contents is acquired from shared disk.

The content of each file and the output format are not publicized.

Archive file	Output result
*output-destination-file-specified-in-dir-option**archive-file-name-specified-in-arc-option*_64.jar	- All files under ***installation-destination-folder-of-JP1/OA***\logs - All files under ***installation-destination-folder-of-JP1/OA***\conf - All files under ***installation-destination-folder-of-JP1/OA***\work - All files under ***installation-destination-folder-of-JP1/OA***\data - All files under ***installation-destination-folder-of-JP1/OA***\system\HDB\SPOOL - Execution result of ***installation-destination-folder-of-JP1/OA***\system\HDB\BIN\pdinfoget.bat - All files under ***Windows-folder*** [#1]\Temp\jp1common - All files under ***Windows-folder***[#1]\Temp\ HITACHI_JP1_INST_LOG - All files under ***Windows-folder*** [#1]\Temp\ HITACHI_HICOMMAND_INST_LOG - ***ProgramFiles(x86)-folder***[#2]\InstallShield Installation Information\{747530F5-28CD-43B5-8D6F-F78A9874864F}\setup.ini - ***ProgramFiles(x86)-folder***[#2]\InstallShield Installation Information\{747530F5-28CD-43B5-8D6F-F78A9874864F}\setup.plg - ***ProgramFiles-folder***[#3]\Hitachi\jp1_common\jp1oa - List of files under the installation destination of JP1/OA - List of registry keys under HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\

Archive file	Output result
	- hosts file - services file - Execution result of the ipconfig command of the OS - Execution result of the netstat command of the OS - Execution result of the msinfo32 command of the OS - Execution result of the systeminfo command of the OS - Execution result of the common component's material collection tools (hcmds64getlogs)
*output-destination-file-specified-in-dir-option**archive-file-name-specified-in-arc-option*_64.hdb.jar	Execution result of the common component's material collection tool (hcmds64getlogs)
*output-destination-file-specified-in-dir-option**archive-file-name-specified-in-arc-option*_64.db.jar	Execution result of the common component's material collection tool (hcmds64getlogs)
*output-destination-file-specified-in-dir-option**archive-file-name-specified-in-arc-option*_64.csv.jar	Execution result of the common component's material collection tool (hcmds64getlogs)

#1: By default, `C:\WINDOWS` is used as the Windows folder.

#2: By default, `C:\Program Files (x86)` is used as the ProgramFiles(x86) folder.

#3: By default, `C:\Program Files` is used as the ProgramFiles folder.

Storage location

installation-destination-folder-of-common-component\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- Do not interrupt the execution of this command.
- If execution of this command is interrupted, the hcmds64getlogs command stops because the folder specified in the dir option has insufficient free space. Secure a sufficient amount of space in the folder specified in the dir option, and then re-execute this command. The following is the amount of required free space:

For non-cluster systems:

Capacity of folders and files under ***installation-destination-folder-ofJP1/OA***\data + capacity of folders and files under ***installation-destination-folder-of-JP1/OA***\logs + 40 GB

For cluster systems:

Size of folders and files in ***shared-folder-name***\Analytics\data + size of folders and files in ***installation-destination-folder-of-JP1/OA***\logs + size of folders and files in ***shared-folder-name***\Analytics\logs + 40 GB

If products that use the common component are included, add the capacity required for collecting log information for these products in the calculation.

- Do not execute more than one instance of this command at the same time.
- If you use the same option more than once, the option specified first is used.

- If you do not need to acquire information stored in databases of JP1/OA, set the following environmental variable before executing the command:

  Variable name: GETDBDATA Value: SKIP
- If you are using JP1/OA in a cluster configuration, execute this command on both the active and standby hosts.
- You can execute this command even if the JP1/OA server is not running. For this reason, even if a failure occurs in the cluster configuration, you can still collect log information without performing a failover to the other server.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	The command finished abnormally.

Example

The following example shows the use of this command to collect log information in the specified file:

hcmds64getlogs /dir "C:\Users\folder01" /types Analytics /arc OA_log

7.8.4 joanodecount (shows the number of management nodes)

Functionality

This command shows the number of management nodes of JP1/OA.

Format

joanodecount

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
14	You do not have permission to execute this command.
42	A communication error (failure to acquire the number of management nodes) occurred.
84	The argument is invalid.
86	Connection to the JP1/OA service failed.
127	An unexpected error occurred.
Other than above	The command finished abnormally.

7.8.5 restoresystem (restore the JP1/OA system)

Functionality

This command restores the backup for JP1/OA settings or database information data that you acquired by executing the backupsystem command.

Format

restoresystem

/dir ***backup-directory***

/type {all | Analytics}

[/auto]

Arguments

/dir***backup-directory***

Specify the folder in which the backup data is stored, in absolute or relative path format.

/type {all | Analytics}

Specify the type of information for backup.

- all

  Restores information of JP1/OA and the common component.

  The common component manages the user information.

- Analytics

  Restores information of JP1/OA only.

/auto

Automatically stops or starts services and databases of JP1/OA and products that use the common component. If you omit this option, these services and databases are not stopped or started automatically.

Storage location

installation-destination-folder-of-JP1/OA\bin

Execution permissions

The Administrator permission is required to perform this operation.

Notes

- When restoring the backup, the folder in which the backup file is stored requires 2 GB of free space.

- The following files are not restored by this command. If necessary, manually re-set or relocate the files.

  (1) Files that require re-settings

  - Configuration file for linkage with external authentication servers (exauth.properties)
  - Security definition file (security.conf)
  - Configuration files for changing port numbers (httpsd.conf, user_httpsd.conf, hsso_httpsd.conf, user_hsso_httpsd.conf)

  The above files are backed up in the following folders:

  - ***backup-folder***\HBase\base\conf
  - ***backup-folder***\HBase\base\httpsd.conf

  (2) Files that require relocation

  Files for https connections are defined in the httpsd.conf file and the user_httpsd.conf file. Place the files in their respective storage locations.

  - SSL server certificate file for https connections
  - Private-key file for https connections

- If you do not specify the auto option, stop the service by executing the hcmds64srv command with the stop option specified. The service to be stopped depends on the specification of the type option.

  If you specified all in the type option:

  You need to stop not only the service of JP1/OA, but also the services of the products that use the common component.

  If you specified Analytics in the type option:

  You need to stop the service of JP1/OA only.

- Make sure that the following information is the same between the environment where the backup was acquired and

the environment where the information was restored:

(1) Version of JP1/OA

(2) Installation directory of JP1/OA

(3) Database storage directory of JP1/OA

- In an environment where JP1/OA coexists with JP1/AO, if you perform a restoration by specifying "all" in the type option, the definition information for the common component is also restored. In this case, an inconsistency might occur in the definition information between the products that use the common component and the common component. Therefore, to restore the backup in an environment where JP1/AO and products that use the common component coexist with JP1/OA, perform the restoration by using any of the following procedures:

(1) To restore data for products that use the common component, in addition to JP1/OA data

1. Execute the restore command for the product that uses the common component.
2. Execute the JP1/OA restore command by specifying /type Analytics.

(2) To restore only user information, in addition to JP1/OA data

1. Execute the JP1/OA restore command by specifying /type Analytics.
2. Update the user management information.

(3) To restore data of JP1/OA only

1. Execute the JP1/OA restore command by specifying /type Analytics.

- If a file with the extension ".original" exists under the following folder, change the extension of the file and then execute the command.

For non-cluster systems:

installation-destination-folder-of-JP1/OA\conf

For cluster systems:

shared-folder-name\Analytics\conf

Return values

The following table describes the return values of the command:

Return value	Description
0	The command finished normally.
1	The argument is invalid.
2	Command execution was interrupted.
3	The service status is invalid.
4	Another command is currently executing.
7	The specified path is invalid.
9	The specified path does not exist.
10	The specified path cannot be accessed.
14	You do not have permission to execute this command.
110	Execution of restoration failed.

Return value	Description
111	The start or stop of the service failed.
113	The backup file is invalid.
255	Command execution was interrupted due to an error other than above.

Example

The following example shows the use of this command to restore information of JP1/OA only:

```
restoresystem /dir "C:\Users\Backup" /type Analytics /auto
```

8.Troubleshooting

8.1 Cause and action

8.1.1 Management targets cannot be found.

(1) vCenter cannot be found.

Cause:

VMware authentication has not been configured.

Actions to be taken:

To find vCenter, VMware authentication is needed. Configure VMware authentication for the corresponding server.

(2) FC Switch cannot be found. (When the FC Switch is monitored by the SMI-S provider)

Cause:

The following are possible causes:

- The IP address of FC Switch is being directly retrieved.
- FC Switch is not monitored by the SMI-S provider.

Actions to be taken:

Take the following actions according to the cause:

- Retrieve the IP address of the SMI-S provider.
- Install the SMI-S provider that supports FC Switch to monitor FC Switch.
- Use the following tool to check whether connections to the SMI-S provider can be established:
  installation-destination-folder-of-JP1/OA\bin\system\smisgetenv.bat
  For details about how to use the tool above, see *Appendix H. How to Use the SMI-S Provider Connection Check Tool*. If connections can be established, review the settings of the SMI-S provider.

(3) SMI-S Storage cannot be found.

Cause:

The management IP address of the storage might be in the retrieval process.

Actions to be taken:

- Retrieve the IP address of the SMI-S provider.
- Use the following tool to check whether connections to the SMI-S provider can be established:
  installation-destination-folder-of-JP1/OA\bin\system\smisgetenv.bat
  For details about how to use the tool above, see *Appendix H. How to Use the SMI-S Provider Connection Check Tool*. If connections can be established, review the settings of the SMI-S provider.

(4) WMI connection to the managed server failed.

Cause:

The configuration of the OS is incorrect.

Actions to be taken:

Review the configuration of the Windows firewall, DCOM, and UAC.

(5) SSH connection to the managed server failed.

Cause:

The following are possible causes:

- The configuration of the IP address is incorrect.
- The configuration of the default gateway is incorrect.
- The configuration of Subnet Mask is incorrect.
- The port used for SSH connections is blocked by the firewall.

Actions to be taken:

Confirm that the connection destination information (IP address, default gateway, Subnet Mask) is correct. Additionally, confirm that the configuration of the firewall on the connection destination is correct.

(6) When information is acquired from the managed host through the SSH protocol, the acquisition fails.

Cause:

The following are possible causes:

- The settings to permit the execution of the `su` command without a password are enabled.
- A communication failure occurred.

Actions to be taken:

Take the following action according to the cause:

- Confirm that when you log in to the managed server as a user connecting to JP1/OA and enter the `su - root` command, the system enters the "waiting for password input" state.

  If the system does not enter the "waiting for password input" state, disable the settings to permit the execution of the `su` command without a password.

- Confirm whether a communication failure occurred. If a communication failure occurred, remove the cause of the failure.

(7) There is no problem in the connection state, authentication state, free disk space, and performance, but the state of the IT resources is abnormal.

Cause:

A problem might have occurred in the state of the management target.

Actions to be taken:

Take the following steps to handle the problem:

1. Check whether a state monitoring error event displayed in the **Events** tab reports a component (such as a network adapter) problem.
2. Remove the problem in the component of the corresponding event and recollect information about the target IT resources.

8.1.2 Connection to the GUI of JP1/OA cannot be established.

When you cannot connect to the GUI of JP1/OA, take the following steps to handle the problem.

Operation procedure:

1. Execute the `hcmds64srv` command with the status option specified to check the operation status of JP1/OA.
2. If the services "HAnalytics Engine Web Service" and "HBase 64 Storage Mgmt SSO Service" are running, and the service "HBase 64 Storage Mgmt Web Service" is not running, a port number might be redundant. Check the event log.
3. If the following log is output, review the configuration of ports used by the JP1/OA server:

Element	Contents
Level	Error
Source	HitachiWebServer
Message	The service named HBase 64 Storage Mgmt Web Service reported the following error: >>> (OS 10048)Only one usage of each socket address (protocol/network address/port) is normally permitted. : make_sock: could not bind to address [::]:[*redundant-port-number*]

8.1.3 Login to JP1/OA is unavailable.

When you cannot log in to JP1/OA, use the following methods to review the configuration:

- Confirm that the user ID and password are correct.
- Confirm that the user is registered in JP1/OA.#
- Confirm that required permissions are set for the user.#
- Confirm that the user account is not locked.#

#: These operations need the User Management permission. Ask a user that has the User Management permission to perform these operations to check the configuration.

8.1.4 JP1/OA cannot start.

When JP1/OA cannot start, take the following steps to handle the problem.

1. Confirm that resources such as memory and disk space are sufficient on the JP1/OA server.
2. Confirm that JP1/OA has been installed on the OS and hardware supported by JP1/OA.
   For details about the types of hardware and OSs supported by JP1/OA, see the *Release Notes* of JP1/OA.
3. Execute the `hcmds64srv` command with the status option specified to check the operation status of JP1/OA.
   If the JP1/OA service is not running, start the service.
4. From the web browser, confirm that communication with the JP1/OA server is functioning normally.
5. Confirm that a web browser supported by JP1/OA has been installed. For details about the types of web browsers supported by JP1/OA, see the *Release Notes* of JP1/OA.
6. See the log information and take appropriate actions according to the contents of the error message.
7. If no error message is output to the log information, or the problem is not resolved by the above steps, execute the `hcmds64getlogs` command to collect the log information, and contact the system administrator.

8.1.5 A message indicating that free disk space is insufficient was output to the log.

Cause:

There is not enough space on the disk drive that contains the following folder to perform automatic extension of the database:

For non-cluster systems:

installation-destination-folder-of-JP1/OA

For cluster systems:

shared-folder-name

For details about the messages displayed and reported when this error occurs, use the message ID and see the *JP1/Operations Analytics Messages*.

Actions to be taken:

1. Delete unnecessary files.
2. Increase the capacity of the disk drive (increase the size of disk partitions).

8.1.6 A message indicating that the database is blocked or abnormal was output to the log.

Cause:

An automatic expansion of the database failed because the free space of the disk where the database is stored is insufficient. Consequently, a failure blockage occurs in the database, or the database stops abnormally.

For details about the messages displayed and reported when this error occurs, use the message ID and see the *JP1/Operations Analytics Messages*.

Actions to be taken:

Prepare the backup file that was acquired before the error occurred.

1. Increase the capacity of the disk drive that contains the following folder (increase the disk partitions).

   For non-cluster systems:

   installation-destination-folder-of-JP1/OA

   For cluster systems:

   shared-folder-name

2. After the capacity of the disk drive is increased, restart JP1/OA.
3. If JP1/OA does not start normally, restore JP1/OA according to the procedure in *2.3.3 Restoring data in a JP1/OA system (non-cluster configuration)* or *2.3.4 Restoring data in a JP1/OA system (cluster configuration)*.

8.1.7 An error occurred in the collection result because the time required for collecting information increased significantly.

Cause:

The collection processing might be terminated abnormally because no response is returned from the collection-target resource for a certain period of time.

Actions to be taken:

Check the log and confirm whether an error message indicating that the collection was terminated due to a time-out is output. If such a message is output, check the resource from which no response was returned according to the message, and confirm whether a problem occurred in the resource.

8.1.8 The switch error continues to be displayed in the E2E View window

Cause:

A link-down might be detected for ports that are no longer used due to configuration changes.

Actions to be taken:

In the detailed window for the switch, use the **Assign Normal** button to change the port status to `Normal`. Doing so will make the port status `Normal` until the status changes again, such as when the port is next used.

If the error continues to be displayed, there might be another cause. Re-examine the switch connections again.

8.2 Details of the log information

8.2.1 Log format

Sequence number	Date	Time	rsvd	Program name	pid	tid	ID	Type	Message text	Linefeed code

The following table shows the contents of the log.

Table 8-1 Output elements in a log file

No.	Item name	Contents	Number of bytes
1	Sequence number	Indicates the sequence number of a message	4 bytes
2	Date	Indicates the date when a message is output (in yyyy/mm/dd format)	10 bytes
3	Time	Indicates the time when a message is output (in hh:mm:ss:xxx format). The unit of xxx is milliseconds.	12 bytes
4	rsvd	Indicates blanks in the reserved area	4 bytes
5	Program name	Indicates the program name in 16 or fewer characters. Program names longer than 16 characters will be shortened.	16 bytes
6	pid	Indicates the hash value added to the Runtime instance by JavaVM	8 bytes
7	tid	Indicates the hash value added to the Thread instance by JavaVM	8 bytes
8	ID	Indicates the message ID with a prefix for identifying products	16 bytes
9	Type	Indicates the type of the event that triggered the message output	4 bytes
10	Message text	Indicates free message information	Less than or equal to 4,095 bytes
11	Linefeed code	CRLF: 0x0D, 0x0A	4 bytes

8.2.2 Collecting log information

This section describes the procedure for collecting log information.

Preparation:

Log in to the JP1/OA server by a user that has the Administrator permission of the OS.

Operation procedure:

Execute the `hcmds64getlogs` command. Specify the output destination folder for the dir option.

The log information is output with the following names to the specified output destination folder. However, the contents and output format of these files are not disclosed.

output-destination-folder-name`\HiCommand_log_64.jar`
output-destination-folder-name`\HiCommand_log_64.hdb.jar`
output-destination-folder-name`\HiCommand_log_64.db.jar`
output-destination-folder-name`\HiCommand_log_64.csv.jar`

8.2.3 Details of the event log and public log

(1) Details of event logs

Event logs are output to the location specified in the OS configuration.

You can see event logs by using the Windows event viewer.

(2) Details of public logs

The output destination and file names of public logs are shown below. Public logs are output in WRAP2 format.

Output destination:

installation-destination-folder-of-JP1/OA`\logs`
shared-folder-name`\JP1OA\logs`#

#: This is the output destination of the log if you have installed JP1/OA in a cluster configuration.

File name:

ServiceMessage[n].log

AdapterMessage_[n]_[m].log

RegistryMessage[n].log

Server[n].log

Command_*command-name*[n].log

ServiceCommandMessage[n].log

[n] and [m] are integers.

Appendix A. JP1/OA Services

The following JP1/OA services are registered at the installation of JP1/OA.

Table A-1 JP1/OA services

Service display name	Service name	Startup type	Product
HAnalytics Engine Web Service	AnalyticsWebService	Automatic	JP1/OA
HAnalytics Engine	AnalyticsProcessController	Manual	JP1/OA
HAnalytics Engine Database _OA0	HiRDBEmbeddedEdition_OA0	Manual	JP1/OA
HAnalytics Engine Cluster Database _OA0#	HiRDBClusterService_OA0	Manual	JP1/OA
HiRDB/EmbeddedEdition _HD1	HiRDBEmbeddedEdition_HD1	Automatic	Common Component
HBase 64 Storage Mgmt SSO Service	HBase64StgMgmtSSOService	Automatic	Common Component
HBase 64 Storage Mgmt Web Service	HBase64StgMgmtWebService	Automatic	Common Component
HBase 64 Storage Mgmt Web SSO Service	HBase64StorageMgmtWebSSO Service	Manual	Common Component
HiRDB/ClusterService _HD1	HiRDBClusterService_HD1	Manual	Common Component

#: This service is reserved for use by JP1/OA. The service is not started or stopped and is not used for operation.

Appendix B. Port Numbers Used by JP1/OA

This appendix shows the list of port numbers to be set and directions for firewall passage.

(1) Port numbers used for external connections in JP1/OA

The following table describes the communication services used in JP1/OA to communicate with external systems and the default port numbers.

Table B-1 List of port numbers (used for external connection)

Port number	Access direction through firewall	Exception registration at the time of installation	Description
22015/tcp	Web browser -> JP1/OA	Y	This port is used to access the HBase 64 Storage Mgmt Web Service. The port is also used for the HTTP connection between the JP1/OA server and a web browser.
22016/tcp	Web browser -> JP1/OA	Y	This port is used to access the HBase 64 Storage Mgmt Web Service. The port is also used for the HTTP connection between the JP1/OA server and a web browser.
25/tcp#1	JP1/OA -> SMTP server	N	This port is used to send email messages when specifying conditions of notification settings.
445/tcp	JP1/OA -> JP1/AJS3 server	N	This port is used when JP1/AJS3 is registered by using the method for registering the management software.
445/tcp, 20700/tcp#4, and a dynamic port number is automatically assigned when required#2	JP1/OA -> JP1/IM server	N	This port is used when JP1/IM is registered by using the method for registering the management software.
445/tcp	JP1/OA -> JP1/PFM server	N	This port is used when JP1/PFM is registered by using the method for registering the management software.
443/tcp#3	JP1/OA -> vCenter server	N	This port is used when vCenter is registered by using the method for registering the management software.
135/tcp	JP1/OA	N	This port is used when the monitoring target that uses

Port number	Access direction through firewall	Exception registration at the time of installation	Description
	-> Monitoring target		WMI for monitoring is registered.
A port number that is more than 1024 automatically set by an OS	JP1/OA -> Monitoring target	N	This port is used when the monitoring target that uses WMI for monitoring is registered.
22/tcp#3	JP1/OA -> Monitoring target	N	This port is used when the monitoring target that uses SSH for monitoring is registered.
161/tcp#3	JP1/OA -> Monitoring target	N	This port is used when the monitoring target that uses SNMP for monitoring is registered.
5988/tcp or 5989/tcp#3	JP1/OA -> Monitoring target	N	This port is used when the monitoring target that uses SMI-S for monitoring is registered.

(Legend):

->: The arrow indicates that access direction is from the item on the left to the item on the right in a one-way direction.

Y: Firewall exceptions are registered at the time of installation.

N: Firewall exceptions are not registered at the time of installation.

#1: When specifying the notification settings, you can change the port number in the mail server settings.

#2: The standard range for port numbers that are assigned by the OS are as follows:

Windows Server 2008 or later: 49152 to 65535

#3: When registering the IT resources to be monitored, you can change the port number in the authentication information settings.

#4: This port is used by databese of JP1/IM. If you changed the number of this port, this is the port number set in JP1/IM.

(2) Port numbers used for internal connections in JP1/OA

The following table describes the communication services used by JP1/OA for internal communications and the default port numbers.

Table B-2 List of port numbers (used for internal connection)

Port number	Description
27100/tcp	This port is used for communication between Common Component and the JP1/OA services.

Port number	Description
27101/tcp	This port is used for communication between Common Component and the JP1/OA services.
27102/tcpx or 27102/udp	This port is used for JP1/OA databases.
27103/tcp or 27103/udp	This port is used for JP1/OA databases.
27104/tcp	This port is used among JP1/OA services.
23800/tcp	Used in an embedded database in a cluster configuration

Appendix C. Performance Information Collected by JP1/OA

This appendix describes the performance information collected by JP1/OA.

The following table lists performance information elements collected by JP1/OA.

Table C-1 Performance information to be collected

Resources from which performance information is collected	Performance information	Unit
Windows host	CPU usage[#1]	%
	Memory usage	%
	Average number of received packets on network ports	Packets/sec
	Average number of transmitted packets on network ports	Packets/sec
	Average number of received frames on HBAs	Frames/sec
	Average number of transmitted frames on HBAs	Frames/sec
	Disk reading rate	MBps
	Disk writing rate	MBps
	Average time for the disk transmission processing (Windows)	msec/transfer
	Free disk space	MB
Linux/UNIX host	CPU usage[#1]	%
	Memory usage	%
	Average number of received packets on network ports	Packets/sec
	Average number of transmitted packets on network ports	Packets/sec
	Average number of received frames on HBAs	Frames/sec
	Average number of transmitted frames on HBAs	Frames/sec
	Disk reading rate	MBps
	Disk writing rate	MBps
	Average time for disk transmission processing (Linux/UNIX)	msec/transfer
	Free disk space[#3]	MB
Virtualization software (ESX)	CPU usage	%
	CPU usage for the entire host	%
	Ratio of CPU dispatch wait time	%
	Memory usage	%
	Memory balloon	MB
	Amount of compressed memory	MB

Resources from which performance information is collected	Performance information	Unit
	Speed at which memory is swapped in	MBps
	Speed at which memory is swapped out	MBps
	Average number of transmitted packets on network ports	Packets/sec
	Average amount of received data on network ports	MBps
	Average amount of transmitted data on network ports	MBps
	Disk reading rate	MBps
	Disk writing rate	MBps
	Wait time for disk reading	msec
	Wait time for disk writing	msec
	Wait time for disk commands	msec
	Average number of disk read requests	Transfers/sec
	Average number of disk write requests	Transfers/sec
	Average number of disk command requests	Transfers/sec
	Free disk space[#4]	MB
	Wait time for kernel commands	msec
Virtualization software (Hyper-V)	CPU usage	%
	CPU usage for the entire host	%
	Ratio of CPU dispatch wait time[#2]	%
	Virtual CPU usage for the management OS	%
	Memory usage	%
	Memory balloon	MB
	Average amount of transmitted data on network ports	MBps
	Average amount of received data on network ports	MBps
	Average number of received packets on network ports	Packets/sec
	Average number of transmitted packets on network ports	Packets/sec
	Average number of received frames on HBAs	Frames/sec
	Average number of transmitted frames on HBAs	Frames/sec
	Average number of disk read requests	Transfers/sec
	Average number of disk write requests	Transfers/sec
	Wait time for disk reading	msec
	Wait time for disk writing	msec
	Disk reading rate	MBps
	Disk writing rate	MBps
	Average time for the disk transmission processing (Windows)	msec/transfer

Resources from which performance information is collected	Performance information	Unit
	Free disk space[#4]	MB
Virtual machine	CPU usage for virtual machines	%
	CPU usage for virtual machines	MHz
	Ratio of CPU dispatch wait time for virtual machines	%
	Memory usage for virtual machines	%
	Memory usage for virtual machines	MB
	Memory balloon for virtual machines	MB
	Speed at which memory for virtual machines is swapped in[#5]	MBps
	Speed at which memory for virtual machines is swapped out[#5]	MBps
	Disk usage for virtual machines[#5]	MB
	Disk usage for virtual machines (reserved) [#5]	MB
	Wait time for virtual disk reading	msec
	Wait time for virtual disk writing	msec
	Average number of virtual disk read requests	Transfers/sec
	Average number of virtual disk write requests	Transfers/sec
	Average number of virtual disk read and write requests	Transfers/sec
	Virtual disk reading rate	MBps
	Virtual disk writing rate	MBps
	Average amount of transmitted data on virtual ports	MBps
	Average amount of received data on virtual ports	MBps
	Average number of transmitted packets on virtual ports	Packets/sec
	Average number of received packets on virtual ports	Packets/sec
	Ratio of the average number of transmitted packets that were discarded on virtual ports	%
	Ratio of the average number of received packets that were discarded on virtual ports	%
Volume	Average number of volume read and write requests	IOPS
	Volume reading and writing rate	MBps
	Processing time per volume read and write request	msec/transfer
FC Switch	Average amount of received data on network ports	MBps
	Average amount of transmitted data on network ports	MBps
	Average number of error frames on network ports	Frames/sec
IP Switch	Average number of received packets on network ports	Packets/sec

Resources from which performance information is collected	Performance information	Unit
	Average number of transmitted packets on network ports	Packets/sec
	Average amount of received data on network ports	MBps
	Average amount of transmitted data on network ports	MBps
	Average number of error packets on network ports	Packets/sec

#1

This information element is acquired from the OS. The error might be larger in a virtual environment.

#2

Performance values can be acquired only when the following Hyper-V products are monitored.

- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V

#3

The performance information of free space for disks of UNIX-based OSs is only displayed when management targets are mounted so that their mount points can be read and written. For the free space of the disk of a management target that is mounted so that the mount point can only be read, the performance icon is in a state that is unknown and the performance information is not displayed.

#4

In threshold judgment for free disk space, if the total capacity of the disk is smaller than the warning threshold, the performance state is displayed as unknown. When free disk space is not monitored, you must set the disk not to be monitored. To start monitoring, review the configuration of the monitoring profile.

For example, use a monitoring profile in which the warning threshold is set to 1,000 megabytes to monitor the performance information of a host such as Windows Server 2008 R2 whose system area is about 100 megabytes. In this case, the performance state is displayed as unknown.

#5

Performance values can be acquired only when the virtualization software is ESX.

Appendix D. List of resources managed by JP1/OA

This appendix describes the resources to be managed by JP1/OA.

(1) Applications

The following table shows the products required for managing the applications.

Table D-1 Products required for managing the applications

Product name		Version
JP1/AJS3	JP1/Automatic Job Management System 3	10-00 or later
JP1/IM #	JP1/Integrated Management	10-00 or later
JP1/PFM	JP1/Performance Management	10-00 or later

#

Linking of JP1/IM - View to the **E2E View** window of JP1/OA is supported in JP1/IM versions 09-50 or later.

(2) Virtualization software

The following table shows the virtualization software that can be set as management targets.

Table D-2 Virtualization software that can be set as management targets

Product name		Version
VMware	vCenter Server #1, #2	5.5, 6.0
Hyper-V	Windows Server 2008 R2 Hyper-V	-
	Windows Server 2012 Hyper-V	-
	Windows Server 2012 R2 Hyper-V	-
	Windows Server 2016 Hyper-V	-

(Legend)

-: Not applicable

#1

For details about interoperability between vCenter Server and VMware ESXi, see relevant documents.

#2

In JP1/OA, the following versions of VMware ESXi can be set as the management targets of vCenter Server:

Product name	Version
VMware ESXi	5.0, 5.1, 5.5, 6.0

(3) Host

The following table shows the hosts that can be set as management targets.

Table D-3 Hosts that can be set as management targets

OS name		Edition
Windows	Windows Server 2008 R2#	Standard Enterprise Datacenter
	Windows Server 2012#	Standard Datacenter
	Windows Server 2012 R2#	Standard Datacenter
	Windows Server 2016#	Standard Datacenter
Linux	Red Hat Enterprise Linux 6	32-bit x86 64-bit x86_64
	Red Hat Enterprise Linux 7	64-bit x86_64
	SUSE Linux Enterprise Server 11	64-bit x86_64
	SUSE Linux Enterprise Server 12	64-bit x86_64
	CentOS 6	32-bit x86 64-bit x86_64
	CentOS 7	64-bit x86_64
	Oracle Linux 6	32-bit x86 64-bit x86_64
	Oracle Linux 7	64-bit x86_64
AIX	AIX 6.1	POWER6 POWER7 POWER8
	AIX 7.1	POWER6 POWER7 POWER8
HP-UX	HP-UX 11iv3	IPF
Solaris	Solaris 10	SPARC
	Solaris 11	SPARC

#

This OS does not support environments where Server Core or Nano Server is installed.

(4) IP Switch

To specify an IP Switch as a management target, the corresponding IP Switch must satisfy all the conditions shown in the following table.

Table D-4 Conditions for IP Switches that can be specified as management targets

Conditions	Description
SNMPv1, v2c, or v3	One of SNMP v1, v2c, or v3 is implemented, and SNMP is available.
MIB-II	MIB information defined in RFC 1213, such as `system` or `interfaces`, is implemented.
Bridge MIB	MIB information defined in RFC1493 is implemented.

(5) FC Switch

To specify an FC Switch as a management target, the corresponding FC Switch must satisfy all the conditions shown in table D-5 or table D-6.

When monitoring from SNMP:

Table D-5 Conditions for FC Switches that can be specified as management targets (when monitoring from SNMP)

Conditions	Description	Applicable vendors			
		Brocade	QLogic	Cisco	Other
SNMPv1, v2c, or v3	One of SNMP v1, v2c, or v3 is implemented, and SNMP is available.	--	--	--	--
MIB-II	MIB information defined in RFC 1213, such as `system` or `interfaces`, is implemented.	Y	Y	Y	Y
FCMGMT-MIB (FA-MIB)	MIB information defined in `draft-ietf-ipfc-fcmgmt-int-mib-07` is implemented.	Y	Y	Y	Y
FIBRE-CHANNEL-FE-MIB	MIB information defined in RFC 2837 is implemented.	Y	Y	Y	Y
ENTITY-MIB	MIB information defined in RFC 2737 is implemented.	Y	N	Y	Y
IF-MIB	MIB information defined in RFC 2863 is implemented.	N	N	Y	N
CISCO-IMAGE-MIB	--	N	N	Y	N
CISCO-FSPF-MIB	--	N	N	Y	N
CISCO-FC-FE-MIB	--	N	N	Y	N
CISCO-ZS-MIB	--	N	N	Y	N

(Legend)

Y: Supports MIB information N: Does not support MIB information

When monitoring from SMI-S:

Table D-6 Conditions for FC Switches that can be specified as management targets (when monitoring from SMI-S)

Conditions	Description
SMI-S 1.3 or later	The FC Switch supports version 1.3 or later of SMI-S.

(6) Storage

To specify storage as a management target, the corresponding storage must satisfy all the conditions shown in the following table.

Table D-7 Conditions for storage that can be specified as management targets

Conditions	Description
SMI-S 1.3 or later	The storage supports version 1.3 or later of SMI-S.

Appendix E. List of Limits

The following table lists various limits for JP1/OA.

Table E-1 List of limits for JP1/OA

Item	Limit
Number of users	30
Number of authentication information items	1,000
Number of retrieval ranges that can be added	1,000
Number of consumers	1,000
Number of assignment rules for resources to be assigned to consumers	1,000
Number of conditions that can be set for assignment rules for resources to be assigned to consumers	10
Number of user resource monitoring threshold profiles	1,000
Number of assignment rules for user resource monitoring threshold profiles	1,000
Number of system resource monitoring threshold profiles	1,000
Number of delivery condition profiles	100
Number of delivery email addresses	100
Number of events that can be retained	1,000,000#1
Period for which events can be retained	126 days
Total number of resources that can be displayed in the **E2E View** window	30,000
Number of resources that can be specified for base points in the **E2E View** window	100
Number of actions that can be registered in the list of actions	1,000
Period for which performance information can be retained	126 days#2

#1

When the number of events exceeds the maximum, the oldest 100,000 events are deleted.

#2

For the latest 48 hours, values collected at the collection interval are retained. For performance information older than the latest 48 hours, only values that are summarized to averages for each hour are retained and values collected at the collection interval are not retained.

The following table shows the display period and targets for performance information collected by JP1/OA.

Table E-2 Display period and targets for performance information collected by JP1/OA

Display period	Display target
Latest 1 hour	Values collected at the collection interval
Latest 6 hours	Values collected at the collection interval
Latest 12 hours	Values collected at the collection interval
Latest 24 hours	Values collected at the collection interval

Display period	Display target
Latest 48 hours	Values collected at the collection interval
Latest 7 days	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour
Latest 14 days	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour
Latest 1 month	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour
Latest 2 months	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour
Latest 3 months	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour
Latest 4 months	**Averages** Values that are summarized to averages for each hour **Worst values** Worst values of collected information for each hour

Appendix F. Format for Output of Resource Information to CSV Files

This appendix describes the format used when information about managed resources is output to CSV files.

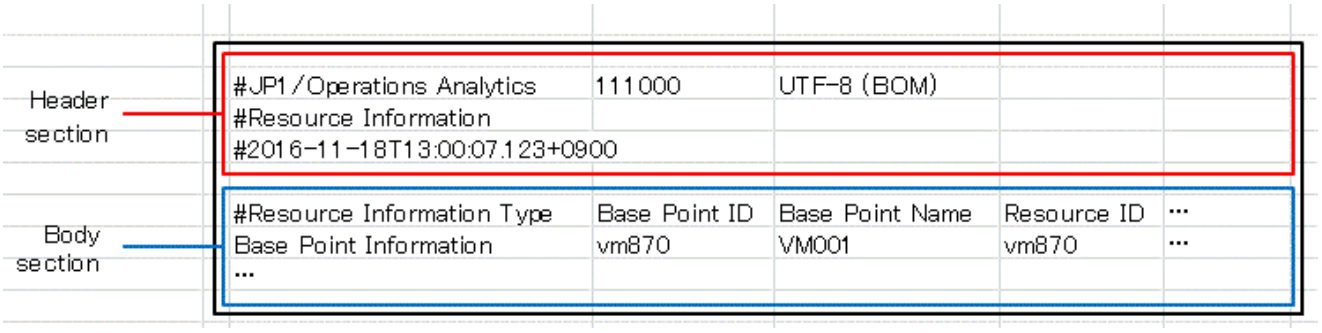
Appendix F.1 CSV file format

CSV files use a comma (,) to delimit items. Commas and newlines included in the value of each item are processed as follows:

- If a comma is included in the value of an item, the entire value is enclosed in double quotation marks (").
- If a newline is included in the value of an item, the newline is replaced with <\n>.
- If the character string <\n> is included in the value of an item, the string is enclosed in double quotation marks (").

Appendix F.2 Structure for CSV files produced when resource information is output

CSV files consist of header and body sections.



(1) Structure of the header section

The same header section is output to all files. The following table describes the structure of the header section.

Table F-1 Structure of the header section

Output row	Output item
First row	The product name `JP1/Operations Analytics` is always output.
First row	The format version of the file
First row	The character encoding This is always `UTF-8 (BOM)`.
Second row	The type of file - `Resource Information`: Basic information - `Latest Performance Information`: Performance information (the most recent values) - `Time Series Performance Information`: Performance information (in chronological order) - `Event Information`: Event information
Third row	When the file was output (the time on the machine where JP1/OA is running)

(2) Structure of the body section: Basic information

The following table describes the structure of the body section when basic information for a managed resource is output.

Table F-2 Structure of the body section showing basic information

Output sequence	Output item	Output information
1	Resource Information Type	One of the following values is output depending on the information to be output: - `Base Point Information`[#1]: For information on the base point resources and node information - `Related Resource Information`[#2]: For information on related resources - `IP Network Information`[#2]: For IP network information - `FC Network Information`[#2]: For FC network information - `Disk Information`: Disk[#2]: For disk information - `File System Information`[#2]: For file system information - `Virtual Disk Information`[#2]: For virtual disk information - `Port Information`[#2]: For port information - `JP1/PFM - Manager Information`[#2]: For JP1/PFM - Manager information - `Execution Agent List`[#2]: For JP1/AJS3 - Agent information #1: The number of rows that are output as is the same as the number of specified base point resources. #2: This value is not output if the base point resource does not have the corresponding information. If the base point resource has multiple information items, the number of rows that are output is the same as the number of information items.
2	Base Point ID	The base point resource ID
3	Base Point Name	The base point resource name
4	Resource ID	The resource ID
5	Resource Name	The resource name
6	Resource Type	The resource type
7	Parent Resource ID	The parent resource ID
8	Parent Resource Name	The parent resource name
9	Parent Resource Type	The parent resource type
10	Display Status	The display status - `Normal`: The resource is not Selected, Highlighted, or Additional. - `Selected`[#]: The resource is selected in the **E2E View** window. - `Highlighted`[#]: The resource is highlighted. - `Additional`: The resource is additional information (the resource is not displayed in the **E2E View** window, but it is output as a component). #: This display status is output only when CSV files are output by using the GUI.
11	Status	The status
12	Power Status	The power status

Output sequence	Output item	Output information
13	Vendor	The vendor
14	Operating System	The operating system
15	Processor	Processor details
16	Memory	Memory details
17	Hypervisor Type	The hypervisor type
18	Model	Model details
19	Cluster	Cluster details
20	Host Name	The host name
21	UUID	The UUID
22	Collector Name	The collector name
23	Collector Access Point	Collector access point details
24	HA Enabled	Whether HA (High Availability) is enabled
25	DRS Enabled	Whether DRS (Distributed Resource Scheduler) is enabled
26	Serial Number	The serial number
27	Firmware	Firmware details
28	Management IP address	The management IP address
29	Number of ports	The number of ports
30	Subnet	The subnet
31	Fabric	The fabric
32	Capacity	Disk capacity details
33	IP Address	IP address details
34	Consumer Name	The consumer name
35	Grade	The grade
36	Classification Label	The classification label
37	Description	Description details
38	System Resource Threshold Profile	The system resource threshold profile
39	User Resource Threshold Profile	The user resource threshold profile
40	Configuration Update	Configuration update details
41	Performance Update	Performance update details
42	Event Update (Application)	Event update details (applications)
43	Adapter	Adapter details
44	Mac Address	MAC address details
45	WWN	WWN details
46	Adapter Number	The adapter number
47	Bus ID	The bus ID
48	Target ID	The target ID
49	LUN ID	The LUN ID
50	Category	Category details
51	Total Capacity	Total capacity details
52	File System	File system details
53	Type	Type details
54	Disk Name	The disk name
55	IF Index	IF index details
56	Port Index	Port index details
57	Port WWN	Port WWN details
58	Service ID	The service ID
59	Product Name	The product name
60	Instance Name	The instance name
61	Monitoring Target	The monitoring target name
62	Execution Agent Name	The execution agent name
63	Maximum Number of Concurrently Executable Jobs	The maximum number of concurrently executable jobs
64	Execution Agent Group Name	The execution agent group name

Output sequence	Output item	Output information
65	Application Type	The application type
66	Custom Application Type	The custom application type

(3) Structure of the body section: Performance information (the most recent values)

The following table describes the structure of the body section when performance information (the most recent values) is output for a managed resource.

Table F-3 Structure of the body section showing performance information (the most recent values)

Output sequence	Output item	Output information
1	Resource ID	The resource ID
2	Resource Name	The resource name
3	Resource Type	The resource type
4	Parent Resource ID	The parent resource ID
5	Parent Resource Name	The parent resource name
6	Parent Resource Type	The parent resource type
7	Performance ID	The performance information ID
8	Metric Name	The metric name
9	Metric Type	The metric type
10	Unit	Unit details
11	Status	The resource status
12	Threshold Value (Warning)	The threshold value (warning)
13	Threshold Value (Error)	The threshold value (error)
14	Condition	The direction of the threshold value - `Greater than`: A larger value indicates a less desirable condition. - `Less than`: A smaller value indicates a less desirable condition.
15	Time	The time
16	Performance Value (Latest)	The performance value (the most recent value)

(4) Structure of the body section: Performance information (in chronological order)

The following table describes the structure of the body section when performance information (in chronological order) is output for a managed resource.

Table F-4 Structure of the body section showing performance information (in chronological order)

Output sequence	Output item	Output information
1	Resource ID	The resource ID
2	Resource Name	The resource name
3	Resource Type	The resource type
4	Parent Resource ID	The parent resource ID
5	Parent Resource Name	The parent resource name
6	Parent Resource Type	The parent resource type
7	Performance ID	The performance information ID
8	Metric Name	The metric name
9	Metric Type	The metric type
10	Unit	Unit details

Output sequence	Output item	Output information
11	Status	The resource status
12	Threshold Value (Warning)	The threshold value (warning)
13	Threshold Value (Error)	The threshold value (error)
14	Condition	The direction of the threshold value - `Greater than`: A larger value indicates a less desirable condition. - `Less than`: A smaller value indicates a less desirable condition.
15	Time	The time
16	Performance Value (Average)	Performance value (average value)
17	Performance Value (Peak)	Performance value (worst value)

(5) Structure of the body section: Event information

The following table describes the structure of the body section when event information is output for a managed resource.

Table F-5 Structure of the body section showing event information

Output sequence	Output item	Output information
1	Event ID	The event ID
2	Device ID	The device ID
3	Device Name	The device name
4	Device Type	The device type
5	Component ID	The component ID
6	Component Name	The component name
7	Component Type	The component type
8	Application Type	The application type
9	Date Time	The registration date and time
10	Level	Level details
11	Status	Status details
12	User	User details
13	Category	The category
14	Message	Message details
15	Device Change Type	Type of change made to the device
16	Component Change Type	Type of change made to the component
17	Attribute Type	Attribute type details
18	Previous Changed Date	The date and time when the previous inventory was obtained
19	New	After the change
20	Previous	Before the change
21	Target Metric Name	The item to be monitored
22	Custom Application Type	The custom application type

Appendix G. Format for Input/Output of Setting Information to CSV Files

This appendix describes the format of CSV files used by the following commands that manipulate setting information.

- addconsumers (create consumer)
- listconsumers (obtain the list of consumers)
- updatecredentials (edit authentication information)

Appendix G.1 CSV file format

CSV files use a comma (,) to delimit items. Any lines starting with a hash mark (#) in an input file are treated as a comment.

When creating a CSV file for input, save it using the UTF-8 character encoding.

Appendix G.2 Structure of the header part of a setting information output file

The following table describes the structure of the header section.

Table G-1 Structure of the header section

Output row	Output item
First row	The product name `JP1/Operations Analytics` is always output.
First row	The format version of the file
First row	The character encoding This is always `UTF-8 (BOM)`.
Second row	The type of file `-Consumer Information`: Consumer Information
Third row	When the file was output (the time on the machine where JP1/OA is running)

Appendix H. How to Use the SMI-S Provider Connection Check Tool

This appendix describes how to use the SMI-S provider connection check tool.

(1) Functionality of the tool

If an SMI-S storage device or FC switch monitored by the SMI-S provider cannot be found, you can use this tool to check whether connections to the SMI-S provider can be established. If connections to the SMI-S provider can be established, take action according to the execution result.

(2) Location of the tool

The following is the location of the tool:

installation-destination-folder-of-JP1/OA\bin\system\smisgetenv.bat

(3) How to use the tool

To use the tool, you must be a member of the Administrators group.

1. Start the administrator console.

   For Windows Server 2008

   (1). In the **Start** menu, select **All Program**, **JP1_Operations Analytics**, and then **Analytics Command**.

   For Windows Server 2012

   (1). From Desktop, display the Start Screen.

   (2). Right-click the Start Screen to display **All Applications**.

   (3). In the **JP1_Operations Analytics** folder, select **Analytics Command**.

   For Windows Server 2016

   (1). Open the Start menu.

   (2). In the **JP1_Operations Analytics** folder, select **Analytics Command**.

2. From the command prompt that opens, execute smisgetenv.bat, which is located in the folder in (2).

For the arguments to be specified in the command, see the following:

<<usage>>

smisgetenv <SMI-S Provider URL> <namespace> <UserID> <Password>

<SMI-S-provider-URL>: URL of the SMI-S provider. The details are as follows:

For SSL communication: https://<IP-address>:<port-number>

For non-SSL communication: http://<IP-address>:<port-number>

<namespace>: Namespace required for the connection

<user-ID>: User ID set in the SMI-S provider

<password>: Password for the user ID

In addition, for the JAVA_HOME environment variable, set the directory of the JDK installed as a common component.
By default, the following directory is set:
Common-Component-installation-folder\uCPSB\hjdk\jdk\jre\bin

(4) Example of using the tool

C:\Program Files\HITACHI\JP1OA\bin\system>smisgetenv.bat
https://xxx.xxx.xxx.xxx:5989/ root/smis/current user1 password1

(5) Examples of output from the tool

(a) Normal termination

Connecting to ... "https://xxx.xxx.xxx.xxx:5989/ root/smis/current"
Connection OK
Completed. <Time: 7820ms>

(b) Abnormal termination

Connecting to ... "https://xxx.xxx.xxx.xxx:5989/ root/smis/current"
Connection NG
Namespace root/smis/currentx is invalid.
The following error occurred.
[getArrayRegisteredProfile] javax.wbem.WBEMException[CIM_ERR_INVALID_NAMESPACE]:
Namespace root/smis/currentx is invalid.
[getEnumerateClassNames] javax.wbem.WBEMException[CIM_ERR_INVALID_NAMESPACE]:
Namespace root/smis/currentx is invalid.
Completed. <Time: 8726ms>

Action to be taken for an abnormal termination:
You can determine the possible cause of an error from the keyword in the error message. The following shows keywords and possible causes:

- CIM_ERR_ACCESS_DENIED
  Cause:
  The specified user ID or password might be incorrect.
- CIM_ERR_INVALID_NAMESPACE
  Cause:
  The specified namespace might be incorrect.
- CIM_ERR_FAILED

Cause:

The specified connection destination or port number might be incorrect.

The overall settings, such as the destination and other SMI-S provider settings, need to be reviewed.

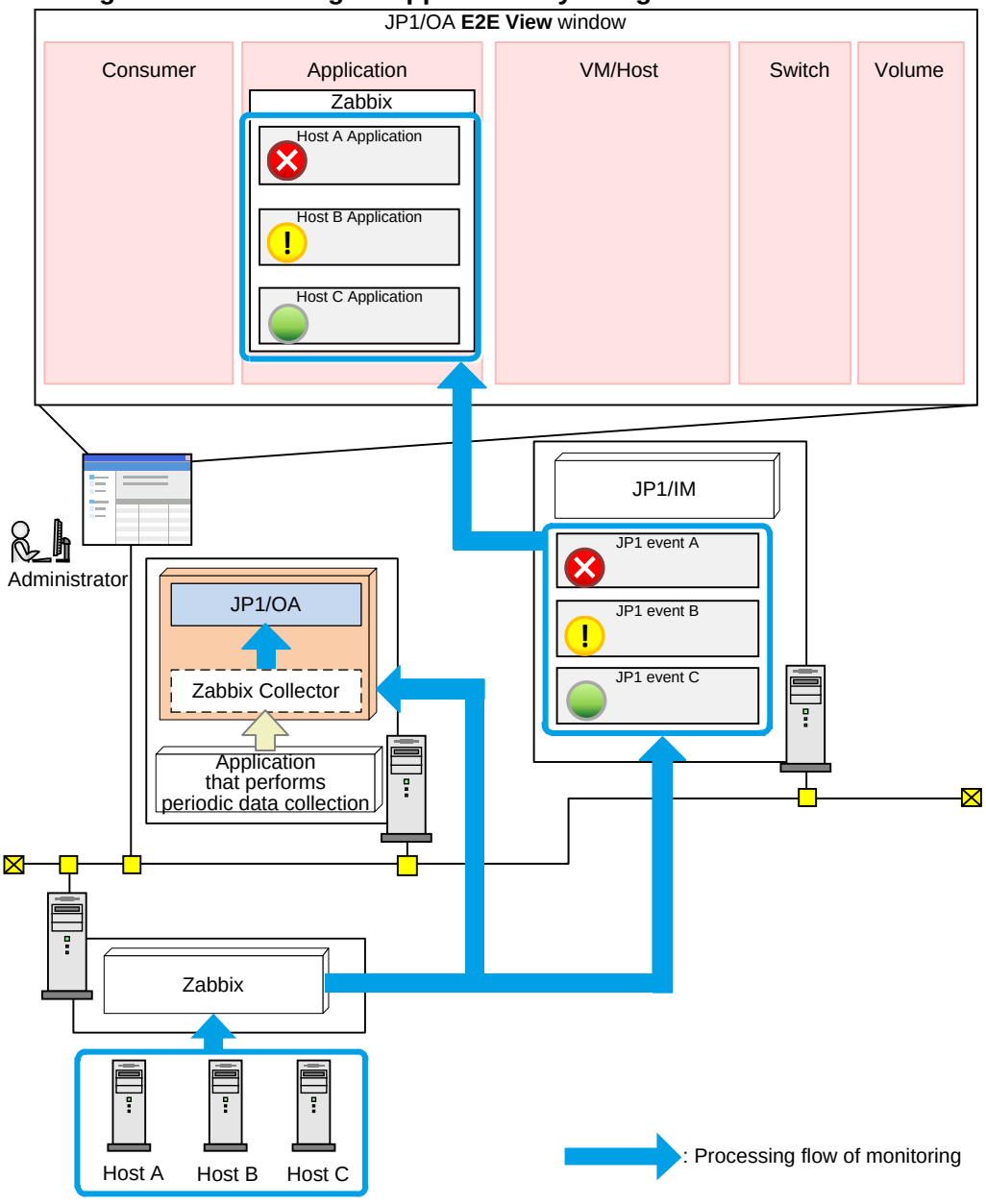
Appendix I. How to Use sample collectors

JP1/OA provides sample collectors that can be used to collect information about applications. This appendix describes the procedure for monitoring applications by using sample collectors.

Appendix I.1 Procedure when using a Zabbix collector

This section describes the procedure for monitoring an application by using the provided sample collector for Zabbix (a Zabbix collector). Add a Zabbix collector as a custom collector in JP1/OA. By periodically executing this collector, information such as host configuration monitored by Zabbix is collected in JP1/OA and can be monitored as an application on JP1/OA. The following figure shows the monitoring of an application by using a Zabbix collector.

Figure I-1 Monitoring an application by using a Zabbix collector



The following table describes the procedure for setting the Zabbix collector. Perform the following operation:

Table I-1 Procedure for setting a Zabbix collector

Step	Setup overview	Refer to:
1	Check the prerequisites	*Appnedex I.3 (1)* *Appnedex I.3 (2)*
2	Set up Zabbix	*Appnedex I.3 (3)*
3	Copy and edit the sample Zabbix collector	*Appnedex I.1 (1)* *Appnedex I.1 (2)*
4	Execute the Zabbix collector and confirm that files have been generated	*Appnedex I.1 (3)*
5	Register the Zabbix collector in JP1/OA	*Appnedex I.1 (4)*
6	Check the displayed application in JP1/OA	*Appnedex I.1 (5)*
7	Set up periodic collection by the Zabbix collector	*Appnedex I.1 (6)*

(1) Copy the sample collector files for Zabbix

JP1/OA provides sample collector files for Zabbix. Copy and then move the folder that contains the sample collector files (copy the source folder and then move it to the destination folder, as follows).

Source folder:

installation-destination-folder-of-JP1/OA`\sample\collector\zabbix`

Destination folder：

installation-destination-folder-of-JP1/OA`\lib\collector\applicaton`

In a cluster system, copy the sample collector files on both the active server and the standby server.# Similarly, copy the sample collector files to the following folder in the shared folder:

shared-folder-name`\Analytics\lib\collector\application`

#: Even if you obtain a backup by executing the `backupsystem` command on the active server and then performed restoration by executing the `restoresystem` command, the files copied to the standby server will not be restored. Restore them manually if necessary.

For details about the configuration of the destination folder, see *Appendex I.2 (1) Folder configuration and list of files*.

Based on the copied file, edit the definition file for the Zabbix collector to match the user environment.

(2) Edit the definition file (CollectorForZabbix.conf) for the Zabbix collector

Edit the user definition file (`CollectorForZabbix.conf`) to be used for the Zabbix collector.

File

`CollectorForZabbix.conf`

Save the file with UTF-8 encoding.

Storage directory

installation-destination-folder-of-JP1/OA`\lib\collector\application\zabbix\usr\`

Definition application timing

When the Zabbix collector is executed

Content to be specified

Specify the key name and value in a single line.

Lines that begin with parameters other than those indicated in the following table are ignored.

Settings

Key name	Setting description	Setting value	Optional or required	Default value
zabbix_url	Specify the URL for the Zabbix server. Example: `http://`*IP-address-or-host-bname-for-Zabbix-server*`:`*port-number*`/zabbix/`	Any character string	Required	Blank
user_b64enc	Specify the user name for the Zabbix server. Specify a character string encoded by Base64.[#1]	Any character string	Required	Blank
password_b64enc	Specify the password for the Zabbix server. Specify a character string encoded by Base64.[#1]	Any character string	Required	Blank

Key name	Setting description	Setting value	Optional or required	Default value
customApplication_conf	Specify whether to generate the `customApplication.conf` file when the Zabbix collector is executed. Specify `FALSE` to not apply the information to JP1/OA, such as when temporarily changing the Zabbix configuration.	TRUE: Automatically generate the file FALSE: Do not automatically generate the file	Optional	TRUE
customAppGrouping_conf	Specify whether to generate the `customAppGrouping.conf` file when the Zabbix collector is executed. Specify `FALSE` to not change the settings by periodic collection.	TRUE: Automatically generate the file FALSE: Do not automatically generate the file	Optional	TRUE
inventory_property	Specify the inventory field for storing the name of the host monitored by Zabbix. JP1/OA uses this value to associate virtual machines and hosts between Zabbix and JP1/OA. For details about the settings, see *Appendex I.3 (2) Prerequisites for the instance of Zabbix to be monitored*.	Any character string	Optional	name
conf_filepath	Specify the destination folder for storing definition files for cluster systems only. For details about definition files, see *Appendex I.2 (1) Folder configuration and list of files*.	For cluster systems: ***shared-folder-name***`\Analytics\lib\collector\application\zabbix\conf` For non-cluster systems: Blank Specify the key name without double quotation marks (`"`), even if a blank is included.	Optional	Blank

Key name	Setting description	Setting value	Optional or required	Default value
tmp_filepath	Specify the destination folder for storing temporary files for the Zabbix collector for cluster systems only.	For cluster systems: ***shared-folder-name***\Analytics\lib\collector\application\zabbix\tmp For non-cluster systems: Blank Specify the key name without double quotation marks ("), even if a blank is included.	Optional	Blank
log_filepath	Specify the output definition path for log files. If a blank is specified, the log files are output to the file path[#2] for the Zabbix collector. The name of the log file is CollectorForZabbix*n*.log. (*n* indicates the number of faces.)	Any character string Specify the key name without double quotation marks ("), even if a blank is included.	Optional	Blank
log_max_num	Specify the maximum number of log files.	1 to 256	Optional	30
api_timeout	Specify the timeout time (in seconds) for when an API for the Zabbix server is used. Revise the settings according to the user's environment.	An integer greater than or equal to 15	Optional	300
generate_conf_retry_interval	Specify the retry interval (in milliseconds) for when a file generation fails.	An integer greater than or equal to 0	Optional	5000

#1: The following explains how to encode in Base64 by using Powershell. In the "*character-string-to-be-encoded*" area of the following command, enter the character string to be encoded, and then execute the command.

```
echo ([Convert]::ToBase64String(([System.Text.Encoding]::Default).GetBytes("
character-string-to-be-encoded")))
```

#2:

installation-destination-folder-of-JP1/OA\lib\collector\application\zabbix

(3) Execute the Zabbix collector

Perform the following procedure to execute the Zabbix collector.

1. Start PowerShell.
2. Access the folder where the script for the Zabbix collector will be executed.
   The following is an execution example:

   cdΔ"***installation-destination-folder-of-JP1/OA***\lib\collector\application\zabbix"

   Note: Δ indicates a halfwidth space.

3. Execute the script for the Zabbix collector.
   The following is an execution example:
   ./CollectorForZabbix.ps1

4. Confirm that the files below were generated.
   For details about the files, see *Appendex I.2 (1) Folder configuration and list of files*.

   Files to be generated:
   - customApplication.conf
   - customAppGrouping.conf

   Folder where the files are generated:
   For non-cluster systems:
   installation-destination-folder-of-JP1/OA\lib\collector\zabbix\conf
   For cluster systems:
   The folder specified for conf_filepath in the definition file (CollectorForZabbix.conf) for the Zabbix collector.

If the files were not generated, see the log file (CollectorForZabbix*n*.log) and revise the procedure performed in *(1)* and *(2)*. For details about how to check the log file, see *8.2.3 Details of the event log and public log*.

(4) Register the Zabbix collector in JP1/OA

To register the Zabbix collector in JP1/OA, restart JP1/OA or execute the reloadproperty command. Next, from JP1/OA, open the **Custom** tab in the **Management Tool Registration** window to confirm that the registered

Zabbix collector was added.

(5) Confirm that the application was added to JP1/OA

In **Application** in JP1/OA **E2E View** window, confirm that the information of the host monitored by Zabbix that was obtained by executing the Zabbix collector is displayed.

(6) Configure settings for period collection by the Zabbix collector

By periodically executing the Zabbix collector that was registered in *(4)*, you can collect information of the host monitored by Zabbix and monitor that information from JP1/OA. This section describes how to periodically execute the Zabbix collector by using the Windows **Task Scheduler**.

Start the Windows **Task Scheduler** to create a task. In the **Create Task** dialog box, select the **Actions** tab and specify the following items. Specify any other items as necessary. For details about items, follow the Windows **Task Scheduler**.

Item	Setting Value
Actions	Start a program
Program/script	`%SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe`
Add arguments (optional)	-CommandΔ".\CollectorForZabbix.ps1"
the Start in (optional)	***`installation-destination-folder-of-JP1/OA`***`\lib\collector\application\zabbix`

Note: Δ indicates a halfwidth space.

The information of the host monitored by Zabbix that was obtained by periodic execution of the Zabbix collector can be checked from **Application** in the JP1/OA **E2E View** window. To stop the information from being collected by the Zabbix collector, you can stop the processing by performing one of the following operations:

- In the **Task Scheduler**, specify **Disable** for the task execution.
- In the JP1/OA **Management Tool Registration** window, display the **Custom** tab, and then from **More Actions**, select **Disable Scheduling**.

To resume the information collection by the Zabbix collector, you can resume the processing by performing both of the following operations:

- In the **Task Scheduler**, specify **Enable** for the task execution.
- In the JP1/OA **Management Tool Registration** window, display the **Custom** tab, and then from **More Actions**, select **Enable Scheduling**.

Appendix I.2 Folder configuration and list of files for the Zabbix collector

(1) Folder configuration and list of files

The table below shows the Zabbix collector folders and list of files located in the folder where JP1/OA is installed.[#] In a cluster system, Zabbix collectors are located in both the folder where JP1/OA was installed and in the shared folder. However, JP1/OA uses only the files stored in the folder described in the following table. JP1/OA does not use files that have the same name but that are stored in a different location. You can delete such files.

#: ***installation-destination-folder-of-JP1/OA***\lib\collector\application\zabbix

Name	Description	Trigger for generating the file
CollectorForZabbix.ps1	The Zabbix collector	The file is generated when the procedure described in *Appendex I.1 (1) Copy the sample collector files for Zabbix* is performed.
CollectorMeta.conf	Invalid flag for the Zabbix collector For cluster systems: The file is generated in ***shared-folder-name***\Analytics\lib\collector\application\zabbix.	The file is generated when the procedure described in *Appendex I.1 (1) Copy the sample collector files for Zabbix* is performed.
NotAutoCollect	Invalid flag for the Zabbix collector For cluster systems: The file is generated in ***shared-folder-name***\Analytics\lib\collector\application\zabbix.	The file is generated when the automatic update of the Zabbix collector is disabled.
readme.txt	Notes for the Zabbix collector	The file is generated when the procedure described in *Appendex I.1 (1) Copy the sample collector files for Zabbix* is performed.
conf	Folder storing the definition file: For cluster systems: ***shared-folder-name***\Analytics\lib\collector\application\zabbix\conf	The file is generated when the Zabbix collector is executed.
customApplication.conf	File for defining the application to be collected by using the Zabbix collector	The file is generated when the Zabbix collector is executed. For details, see *6.3.2 Defining an application*.

Name	Description	Trigger for generating the file
customAppGrouping.conf	Grouping file of the application. This Zabbix collector groups all of the collected applications into the **Zabbix** group.	The file is generated when the Zabbix collector is executed.
customAppMapping.conf	Definition file for mapping between applications	Create this file as necessary. For details, see *6.4.1 Mapping between applications*.
customAppHostMapping.conf	Definition file for mapping between the application and the host	Create this file as necessary. For details, see *6.4.2 Mapping between applications and hosts*.
customEventMapping.conf	Definition file for mapping between JP1 events	Create this file as necessary. For details, see *6.4.4 Defining mapping target for JP1 events*.
tmp	Destination folder for storing temporary files for the Zabbix collector. For cluster systems: ***shared-folder-name***`\Analytics\lib\collector\application\zabbix\tmp`	The file is generated when the Zabbix collector is executed.
usr	Destination folder for storing user definition files for the Zabbix collector	The file is generated when the procedure described in *Appendex I.1 (1) Copy the sample collector files for Zabbix* is performed.
CollectorForZabbix.conf	User definition files for the Zabbix collector	The file is generated when the procedure described in *Appendex I.1 (1) Copy the sample collector files for Zabbix* is performed.

Appendix I.3 Prerequisites for using Zabbix collectors

This appendix explains the prerequisites for using Zabbix collectors in JP1/OA.

(1) Prerequisites for the environment where the Zabbix collector is executed

The following are the prerequisites of the environment where the Zabbix collector is executed:

- The PowerShell (PSVersion) version must be 3.0 or later.
- JP1/OA must be installed.

(2) Prerequisites for the instance of Zabbix to be monitored

The following are the prerequisites for the instance of Zabbix to be monitored.

(a) Zabbix version

The specifications of the Zabbix API must be equivalent to those of Zabbix version 3.0.

The operation of `CollectorForZabbix.ps1` has been verified for Zabbix versions 3.0 and 3.2.

(b) Setting the inventory field for Zabbix

The name of the host monitored by Zabbix must be stored in the **Name** inventory field for Zabbix.

Note: In the user definition file (`CollectorForZabbix.conf`) for the Zabbix collector, `name` is specified as the default value of `inventory_property`. The definition name `name` is used by the system to indicate the **Name** inventory field. If an inventory field other than the **Name** inventory field is used, change the settings specified in the `inventory_property` of the user definition file (`CollectorForZabbix.conf`).

(c) Character limit

Do not exceed the character below. If exceeded, the processing will be skipped and the host monitored by Zabbix will not be displayed in JP1/OA.

Item	Number of characters
Template name for Zabbix	You can specify from 1 to 64 characters.
Host name for Zabbix	You can specify from 1 to 255 characters.
Name of the host monitored by Zabbix	You can specify from 1 to 255 characters.

(d) Characters that cannot be used

Do not use the following characters in the items listed in *(c) Character limit*.

Double quotation marks (`"`), asterisks (`*`), commas (`,`), slashes (`/`), colons (`:`), semicolons (`;`), left angle brackets (`<`), right angle brackets (`>`), question marks (`?`), vertical bars (`|`), backslash (`\`)

(e) Triggering Zabbix

Do not use the host name item of a different instance to trigger Zabbix.

(f) Templates for Zabbix

Apply the template that contains the item for which the host name of the host monitored by Zabbix was obtained.

(3) Setting Zabbix to be monitored

The following explains the settings that must be configured in Zabbix when a Zabbix host is to be monitored in JP1/OA.

(a) Settings in the Zabbix inventory field

The following is an example of setting the host monitored by Zabbix to be automatically registered to the **Name** inventory field for Zabbix.

1. Login to the Zabbix server.
2. In the **Configuration** tab, select the **Templates** tab, and select a template to specify the item.
3. Select the **Items** tab of the selected template, and then select the **Create item** button to create an item.
   Specify a key in **Key** for obtaining the host name. In **Populates host inventory field**, select **Name**. Specify any other items as necessary according to the item type, etc.

   Definition example1:
   If the item type is **Zabbix agent**:
   Key: `system.hostname`
   Populates host inventory field: name

   Definition example2:
   If the item type is **SNMPv2 agent**:
   Key: sysName**SNMP OID**: 1.3.6.1.2.1.1.5.0
   SNMP community: public
   Populates host inventory field: name

4. In the **Configuration** tab, click the **Hosts** tab, and then select a host that obtains host names.
   If the host has not been created, create the host by clicking the **Create host** button.
5. Click the **Templates** tab of the selected host.
   From **Link new templates**, select the template used to create the item to specify a link.
6. Click the **Host inventory** tab of the selected host, and then select the **Automatic** button.
7. Click the **Items** tab of the selected host.
   confirm that the **Status** column in the template is **Enabled** for the name of the item that was created.
   If the **Status** column is **Disabled**, change to **Enable**.

(b) Setting up the instance of JP1/IM linked with Zabbix

If the instance of Zabbix monitored by JP1/OA is linked with JP1/IM, specify the following settings.

- Specify settings to map the event source host
  From JP1/IM, add the event source host as an extended attribute.

For details about the configuration of JP1/IM, see description about setting event source host mapping in the *JP1/Integrated Management - Manager Configuration Guide*.

(c) Setting up JP1 events to be issued from Zabbix

If JP1/OA is linked with Zabbix, JP1/OA can collect information such as errors that occurred in Zabbix by using JP1 events. To enable JP1 events to be issued from Zabbix, specify the following settings. Specify any other items as necessary.

1. Log in to the Zabbix server.
2. In the **Configuration** tab, click the **Actions** tab. Click the **Create action** button to create a new action.
3. From the displayed window, click the **Operations** tab. Then, from the **Operations** item, select **New**.
4. From the **Operation type** list, select **Remote command**.
5. From the displayed window, in **Target list**, select **New**.
   From the **Target** list, select **Host**, Specify the host name of the JP1/OA server.
6. Specify the settings in **Commands**.
   Specify `E.OBJECT_ID` and `E.JP1_SOURCEHOST` as extended attributes in the argument for the `jevsend` command. The following is an example of executing the `jevsend` command.

   jevsend∆-e∆E.OBJECT_ID={HOST.HOST1}∆-e∆E.JP1_SOURCEHOST={INVENTORY.NAME1}
   Note: ∆ indicates a halfwidth space.

Appendix J. Version Changes

This appendix describes the changes between versions.

(1) Changes in version 11-50

- The HAnalytics Engine Database _OA0 service was added to each procedure for setting up the JP1/OA services in cluster software.
- In the `user_httpsd.conf` file example, the content of the SSLRequiredCiphers directive was changed.
- The `AD.inventory.ipSwitch.portsToRemove` key was added to the system property file (Argus.properties).
- Conditions for writing a definition file to display % were deleted or changed.
- Descriptions of the **Event Analysis View** window and the **Performance Analysis View** window were added for the function for outputting resource information.
- Descriptions of how to import JP1/PFM reports and performance information from other software and to then display the imported performance information in performance graphs were added.
- A description for collecting JP1 events from JP1/IM was added to the procedure for linking with a Windows edition of a JP1 product.
- A procedure for linking with a UNIX edition of a JP1 product was added.
- The following descriptions were added to the descriptions for the email template definition files and the command template definition files:

  - The `SE.template.filter.groups.string` key was added to the settings.

  - `%ANALYTICS_GROUPS%` was added to the list of usable fill character variables.
- Settings for which fill character variables can be used were specified in the explanation of the formats of email template definition files and command definition files.
- Descriptions related to application monitoring were added. In accordance with this, the following additions or changes were made:

  - The descriptions of the arguments and return values for the `addsetting` command, `deletesetting` command, and `updatesetting` command were changed.

  - The items output to CSV files as basic information and event information were added.
- The following changes or additions were made regarding the `reloadproperty` command:

  - The description of the command was changed.

  - Definition files referenced by the command were added.

  - The location of the command was modified.
- SHA512withRSA was added as a specifiable value for the `sigalg` option of the `hcmds64ssltool` command.
- The items and item names in the file output by the `listconsumers` command were changed.
- Notes on the `outputevent` command now specify how to deal with the situation in which a large number of events are output.
- The free capacity required for the temporary directory when the `expandretention` command is executed was changed.
- The names of the log files that can be acquired by the logtypes option of the `hcmds64getlogs` command were

modified.

- The following port numbers used for external connections in JP1/OA were changed:

  - Port number 445/tcp, which was used when registering the monitoring target that uses WMI for monitoring, was deleted.

  - Port number 3389/tcp, which was used when the following software was registered as management software, was deleted:

    - JP1/AJS3
    - JP1/IM
    - JP1/PFM

  - Port number 20700/tcp, which was used when registering JP1/IM, was added.

- The following information was added to Performance Information Collected by JP1/OA.

  - Amount of compressed memory
  - Speed at which memory is swapped in
  - Speed at which memory is swapped out
  - Wait time for kernel commands
  - Speed at which memory for virtual machines is swapped in
  - Speed at which memory for virtual machines is swapped out
  - Disk usage for virtual machines
  - Disk usage for virtual machines (reserved)

- A note on setting Windows Server 2016 as a management target was added.
- The format of the URL of an SMI-S provider, specified when using the SMI-S provider connection check tool, was changed.
- The following output items (in CSV files to which resource information is output) were added to the structure of the body section that indicates basic information:

  - Execution Agent Name
  - Maximum Number of Concurrently Executable Jobs
  - Execution Agent Group Name

- Execution Agent List was added to the information output in Resource Information Type.
- A description of the format of CSV files used by commands that perform setting operations was added.

(2) Changes in version 11-10

- Procedures for upgrade installations were added and changed.
- SSL server certificates that use the elliptic curve cipher (ECC) were added to the SSL server certificates that can be used between a Web browser and JP1/OA via an HTTPS connection.
- The default value of "SE.event.maxEventLogRetentionDays" in the system property file (Argus.properties) was changed.
- A description was added for conditions under which the host name of the virtual machine on which the managed application is running can be automatically acquired.
- A description was added for output function of the resource information.

- The procedure for extending the retention period for performance information was added.
- Windows Server 2016 was added to the supported operating systems, and related descriptions were changed.
- The procedure was added for linking with JP1 products for Windows.
- switches (switch) was added as a type of resource for which searches can be performed, within the elements that can be configured for the direct access URL.
- A description was added for customizing application monitoring.
- The subsection hcmds64checkcerts (checks the expiration date of the SSL server certificate) was added to Building-related commands.
- The following operational commands were added:
  - addconsumers (creates consumer)
  - addsetting (creates configuration information)
  - deletesetting (deletes configuration information)
  - getsettings (obtains configuration information)
  - hcmds64chgurl (changes the URL of JP1/OA)
  - listconsumers (obtains the list of consumers)
  - outputevent (outputs event information to a CSV file)
  - outputlatestperf (outputs performance information (the most recent values) to a CSV file)
  - outputresource (outputs resource information to a CSV file)
  - outputtimeseriesperf (outputs performance information (in chronological order) to a CSV file)
  - updatecredentials (edits authentication information)
  - updatesetting (edits configuration information)
- The subsection expandretention (extends the retention period for performance information) was added to Command list.
- A description was added for using commands to perform operations related to JP1/OA configuration information.
- Volume and Application were added to the values that can be specified for the type option of the listresources command.
- A description was added for conditions under which the SNMP protocol can be used to monitor the FC Switch.
- The subsection The switch error continues to be displayed in the E2E View window was added to Troubleshooting.
- Port numbers that must be used to communicate with JP1/AJS3, JP1/IM, or JP1/PFM were added.
- The following information was added to Performance Information Collected by JP1/OA.
  - CPU usage for virtual machines
  - Memory usage for virtual machines
- Information about applications were added to the List of resources managed by JP1/OA.
- Within the configurable limits for JP1/OA, the values for the following items were changed:
  - Period for which events can be retained
  - Period for which performance information can be retained

(3) Changes in version 11-00

- The procedure for overwrite installation was added and changed.
- The procedure for uninstalling JP1/OA was changed.
- The notes on the user_httpsd.conf file were changed.
- Paths and folders for cluster systems were added and changed.
- The values that can be specified for SE.event.maxCurrentEventResult and SE.cluster.logicalHostName in the system property file (Argus.properties) were changed.
- A description was added to clearly state that ASCII characters are to be specified for EventAction.cmd in the event action definition file.
- The description of the size of backup files was changed.
- The procedure for stopping a JP1/OA system was changed.
- A step for editing keys in the definition file was added to the procedure for changing the port number.
- The procedure for setting the clock of the JP1/OA server backward was deleted.
- The paths to the folders created on the JP1/OA shared disk were changed.
- The note on saving the file was deleted.
- Notes on executing the hcmds64srv command were added.
- The note on starting only JP1/OA services by specifying the server option was changed.
- The notes on the hcmds64getlogs command were changed.
- The description of the response body and response header for the status codes of 4xx and 500 was changed.
- The API status code 404 was deleted from the description of deleting user profiles, deleting system profiles, and deleting consumers.
- The causes and actions to be taken when management targets cannot be found were changed.
- HiRDB/ClusterService _HD1 and HiRDB/EmbeddedEdition _HD0 were added to the JP1/OA services.
- 135/tcp and 445/tcp were added to the port numbers used by JP1/OA. In addition, text was added to clarify that port numbers automatically set by an OS is 1024 or the numbers greater than that.
- The period for which performance information can be retained was changed from 7 days to 14 days. In addition, the time for retaining values collected at collection intervals was changed from 24 hours to 48 hours.
- A description was added to the section describing how to use the SMI-S provider connection check tool.

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