HITACHI
Inspire the Next

JP1 Version 13

JP1/Integrated Management 3 - Manager Command, Definition File and API Reference

3021-3-L06-10(E)

Notices

■ Relevant program products

For details about the supported OS versions, and about the OS service packs and patches required by JP1/Integrated Management 3 - Manager and JP1/Integrated Management 3 - View, see the release notes for the relevant product.

JP1/Integrated Management 3 - Manager (for Windows):

P-2A2C-8EDL JP1/Integrated Management 3 - Manager 13-01

The above product includes the following:

P-CC2A2C-9MDL JP1/Integrated Management 3 - Manager 13-01 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-01 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-01 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-00 (for AIX)

JP1/Integrated Management 3 - Manager (for Linux):

P-842C-8EDL JP1/Integrated Management 3 - Manager 13-01

The above product includes the following:

P-CC842C-9MDL JP1/Integrated Management 3 - Manager 13-01 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, Amazon Linux 2023)

P-CC9W2C-9MDL JP1/Integrated Management 3 - Manager 13-01 (for SUSE Linux 15, SUSE Linux 12)

P-CC2A2C-6HDL JP1/Integrated Management 3 - View 13-00 (for Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10)

P-CC2A2C-9GDL JP1/Integrated Management 3 - Agent 13-01 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-9GDL JP1/Integrated Management 3 - Agent 13-01 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC2A2C-6LDL JP1/Base 13-00 (for Windows Server 2022, Windows Server 2019, Windows Server 2016)

P-CC842C-6LDL JP1/Base 13-00 (for Linux 9, Linux 8, Linux 7, Oracle Linux 9, Oracle Linux 8, Oracle Linux 7, SUSE Linux 15, SUSE Linux 12, Amazon Linux 2023)

P-CC1M2C-6LDL JP1/Base 13-00 (for AIX)

■ Trademarks

HITACHI, HiRDB, JP1 are either trademarks or registered trademarks of Hitachi, Ltd. in Japan and other countries.

AIX is a trademark of International Business Machines Corporation, registered in many jurisdictions worldwide.

This product includes software developed by Andy Clark.

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

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

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

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

■ 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$^{(R)}$
IE	Windows Internet Explorer	Windows$^{(R)}$ Internet Explorer$^{(R)}$
SCVMM		Microsoft$^{(R)}$ System Center Virtual Machine Manager 2008
		Microsoft$^{(R)}$ System Center Virtual Machine Manager 2012
Windows 10		Windows$^{(R)}$ 10 Enterprise 64-bit
		Windows$^{(R)}$ 10 Home 64-bit
		Windows$^{(R)}$ 10 Pro 64-bit
Windows 11		Windows$^{(R)}$ 11 Enterprise
		Windows$^{(R)}$ 11 Home
		Windows$^{(R)}$ 11 Pro

Abbreviation	Full name or meaning
Windows Server 2016	Microsoft(R) Windows Server(R) 2016 Datacenter
	Microsoft(R) Windows Server(R) 2016 Standard
Windows Server 2019	Microsoft(R) Windows Server(R) 2019 Datacenter
	Microsoft(R) Windows Server(R) 2019 Standard
Windows Server 2022	Microsoft(R) Windows Server(R) 2022 Datacenter
	Microsoft(R) Windows Server(R) 2022 Standard

Windows is often used generically to refer to Windows 11, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 10.

■ 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.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

■ Issued

Mar. 2024: 3021-3-L06-10(E)

■ Copyright

Summary of amendments

The following table lists changes in this manual (3021-3-L06-10(E)) and product changes related to this manual.

Changes	Location
Added AIX performance data collection capability (Node exporter for AIX) to performance monitoring function by JP1/IM - Agent. Accordingly, the following commands were added. • jpc_stop_node_exporter_aix (for AIX only) The following definition files were added. • Node exporter for AIX metric definition file • Node exporter for AIX discovery configuration file The explanations were added to the following definition files. • Prometheus configuration file • Alert configuration file • Unit definition file	*1. Lists of commands*, *1. jpc_stop_node_exporter_aix (AIX only)*, *2. List of definition files*, *2. Node exporter for AIX metric definition file (metrics_node_exporter_aix.conf)*, *2. Node exporter for AIX discovery configuration file (jpc_file_sd_config_node_aix.yml)*, *2. Prometheus configuration file (jpc_prometheus_server.yml)*, *2. Alert configuration file (jpc_alerting_rules.yml)*, *2. Unit definition file (jpc_program-name.service)*
Added ability to monitor system log information and CCMS alerting information for SAP systems. Accordingly, the following commands were added. • jr3slget • jr3alget The following definition files were added. • Sample file of Script exporter configuration file for SAP system monitoring • Sample file of system log information monitoring definition file for SAP system • Sample file of CCMS alert information monitoring definitionfile for SAP system • Environment parameters file for jr3slget command • Sample file of environment parameters file for jr3slget command • Environment parameters file for jr3alget command • Sample file of environment parameters file for jr3alget command The explanation was added to the following definition file. • Prometheus configuration file	*1. Lists of commands*, *1. jr3slget*, *1. jr3alget*, *2. List of definition files*, *2. Sample file of Script exporter configuration file for SAP system monitoring (jpc_script_exporter_sap.yml)*, *2. Sample file of system log information monitoring definition file for SAP system (fluentd_sap_syslog_tail.conf)*, *2. Sample file of CCMS alert information monitoring definitionfile for SAP system (fluentd_sap_alertlog_tail.conf)*, *2. Environment parameters file for jr3slget command (jr3slget.ini)*, *2. Sample file of environment parameters file for jr3slget command (jr3slget.ini.sample)*, *2. Environment parameters file for jr3alget command (jr3alget.ini)*, *2. Sample file of environment parameters file for jr3alget command (jr3alget.ini.sample)*, *2. Prometheus configuration file (jpc_prometheus_server.yml)*
Added Oracle Database monitoring facility (OracleDB exporter) to performance monitoring function by JP1/IM - Agent. Accordingly, explanations about OracleDB exporter were added to the following commands. • jimasecret • jpc_service • jpc_service_autostart • jpc_service_start • jpc_service_stop	*1. jimasecret*, *1. jpc_service*, *1. jpc_service_autostart*, *1. jpc_service_start*, *1. jpc_service_stop*, *2. List of definition files*, *2. OracleDB exporter metric definition file (metrics_oracledb_exporter.conf)*, *2. OracleDB exporter default collection metric definition*

Changes	Location
The following definition files were added. - OracleDB exporter metric definition file - OracleDB exporter default collection metric definition file - OracleDB exporter discovery configuration file The explanations were added to the following definition files. - Alert configuration file - Service definition file	*file (default-metrics.toml)*, *2. OracleDB exporter discovery configuration file (jpc_file_sd_config_oracledb.yml)*, *2. Alert configuration file (jpc_alerting_rules.yml)*, *2. Service definition file (jpc_program-name_service.xml)*
Removed the "IM Exporter" section and terminology, and integrated the following features into JP1/IM - Agent or JP1/IM - Manager description. - Windows process data collection capability (Windows exporter) - Linux process data collection capability (Process exporter) - Azure monitor performance data collection capability (Promitor) - UAP monitoring capability (Script exporter) - Log metrics feature (Fluentd) - Container monitoring feature	*2. Definition Files*, *2. List of definition files*
Added Windows and Linux service monitoring capabilities to performance monitoring function with JP1/IM - Agent. Accordingly, the following definition files were added. - Windows exporter (service monitoring) metric definition file - Node exporter (service monitoring) metric definition file The explanations were added to the following definition files. - Alert configuration file - Windows exporter discovery configuration file - Node exporter discovery configuration file - Unit definition file - Windows exporter configuration file	*2. List of definition files*, *2. Windows exporter (Service monitoring) metric definition file (metrics_windows_exporter_service.conf)*, *2. Node exporter (Service monitoring) metric definition file (metrics_node_exporter_service.conf)*, *2. Alert configuration file (jpc_alerting_rules.yml)*, *2. Windows exporter discovery configuration file (jpc_file_sd_config_windows.yml)*, *2. Node exporter discovery configuration file (jpc_file_sd_config_node.yml)*, *2. Unit definition file (jpc_program-name.service)*, *2. Windows exporter configuration file (jpc_windows_exporter.yml)*
The following setting was added to imagent configuration file. - service_startup_wait_time (wait time for service start up in definition file update process)	*2. imagent configuration file (jpc_imagent.json)*
Deleted the description of the cloud service log linkage tool.	--
The AIX version of JP1/Base was added as an agent.	--
The following applicable OS was added: - Amazon Linux 2023	--

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

Preface

This manual describes the commands, definition files and API of JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, and JP1/Integrated Management 3 - Agent systems. In this manual, JP1/Integrated Management is abbreviated to *JP1*, and JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, and JP1/Integrated Management 3 - Agent are generically referred to as *JP1/Integrated Management* or *JP1/IM*. In addition, in this manual, read JP1/Integrated Management - Manager, JP1/Integrated Management - View, and JP1/Integrated Management - Agent as JP1/Integrated Management 3 - Manager, JP1/Integrated Management 3 - View, and JP1/Integrated Management 3 - Agent, respectively.

■ Intended readers

This manual is intended for users who want to manage, use, and operate an infrastructure that manages an open-platform system form JP1/IM. More specifically, it is intended for:

- System administrators who manage, use, and operate JP1/IM to centrally monitor the events that arise in the system.
- System administrators who manage, use, and operate JP1/IM to centrally monitor the status of the system management infrastructure based on correlation with events that arise in the system
- Those who have knowledge of operating systems and applications

■ Organization of this manual

This manual consists of the following chapters:

1. Commands

Chapter 1 describes the syntax for the commands that can be used in JP1/Integrated Management.

2. Definition Files

Chapter 2 describes the formats and syntax of the definition files for JP1/Integrated Management.

3. JP1 Events

Chapter 3 describes the types and attributes of the JP1 events that are issued by JP1/Integrated Management.

4. User-created Plug-ins

JP1/IM - Manager (Intelligent Integrated Management Base) can execute processing by using user-created plug-ins, which will be described in detail in this chapter.

5. API

Chapter 5 describes the APIs provided by JP1/Integrated Management.

6. Customization of Integrated Operation Viewer Window

Chapter 6 describes how to display a user-defined window when a specific IM management node is selected in the Integrated Operation Viewer window.

7. Information Necessary to Use the Intelligent Integrated Management Base

Chapter 7 describes the SIDs and json objects that are necessary to use the Intelligent Integrated Management Base, the adapter command information that is necessary to use user-created plug-ins, and the functionality provided to generate an IM management node tree. It also provides a sample plug-in and details regarding the control characters.

8. Lists of System-Monitoring Objects (for Central Scope)

Chapter 8 describes the system-monitoring objects that are provided by JP1/Integrated Management.

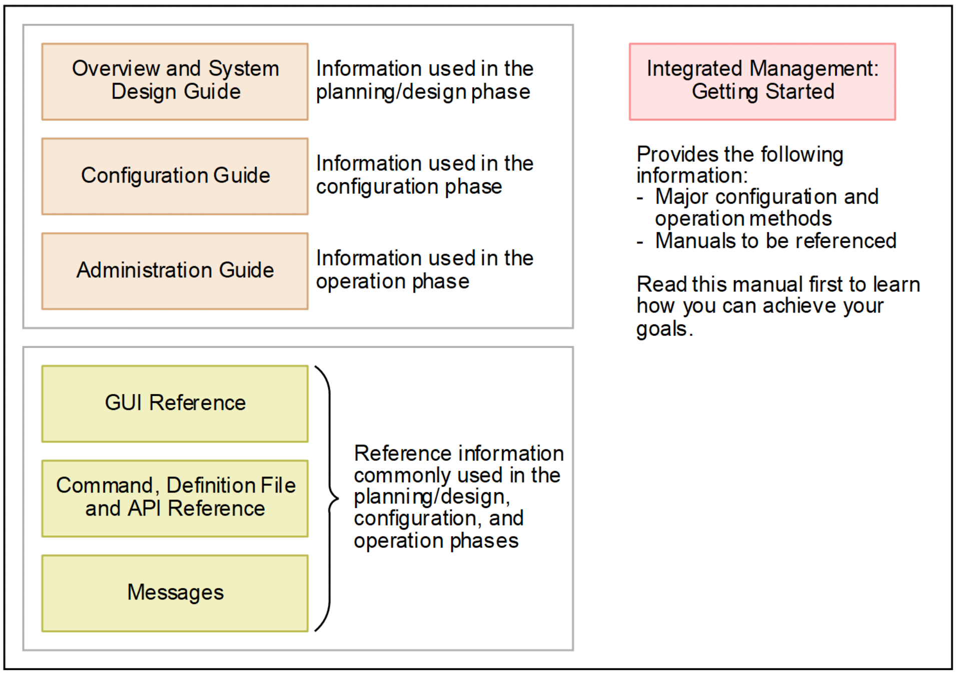
9. Monitoring Tree Models (for Central Scope)

Chapter 9 describes the structures of monitoring trees that are created automatically.

■ Manual suite

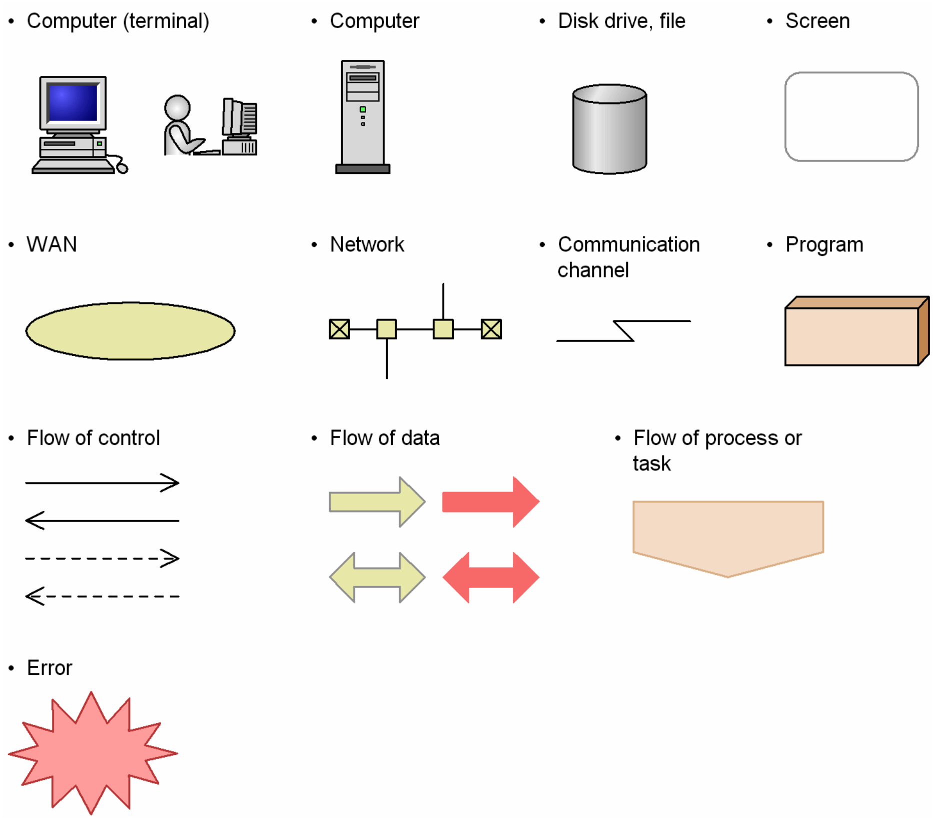
JP1/IM manuals provide necessary information according to the phase in the system life cycle (the phases include planning/design, configuration, and operation). Read the manual appropriate for the purpose.

The following figure explains which phases the JP1/IM manuals provide information for.


Overview and System Design Guide
Information used in the planning/design phase
Configuration Guide
Information used in the configuration phase
Administration Guide
Information used in the operation phase
GUI Reference
Command, Definition File and API Reference
Messages
Reference information commonly used in the planning/design, configuration, and operation phases
Integrated Management: Getting Started
Provides the following information:
- Major configuration and operation methods
- Manuals to be referenced
Read this manual first to learn how you can achieve your goals.

■ Conventions: Diagrams

This manual uses the following conventions in diagrams:



■ 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 explains the symbols used in this manual:

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.
Δ	Indicates a space. Δ_0: Zero or more spaces (space can be omitted). Δ_1: One or more spaces (space cannot be omitted).
▲	Indicates a tab. Example: ▲ `A` means that a tab character precedes `A`.

■ Conventions: Installation folders for the Windows version of JP1/IM and JP1/Base

In this manual, the installation folders for the Windows versions of JP1/IM and JP1/Base are indicated as follows:

Product name	Installation folder	Default installation folder#
JP1/IM - View	*View-path*	*system-drive*`:\Program Files\Hitachi\JP1CoView`
JP1/IM - Manager	*Manager-path*	*system-drive*`:\Program Files\Hitachi\JP1IMM`
	Console-path	*system-drive*`:\Program Files\Hitachi\JP1Cons`
	Scope-path	*system-drive*`:\Program Files\Hitachi\JP1Scope`
JP1/IM - Agent	*Agent-path*	*system-drive*`:\Program Files\Hitachi\JP1IMA`
JP1/Base	*Base-path*	*system-drive*`:\Program Files\Hitachi\JP1Base`

#: Represents the installation folder when the product is installed in the default location. The location represented by *system-drive*`:\Program Files` is determined at the time of installation by an OS environment variable, and might differ depending on the environment.

■ Conventions: Meaning of "Administrator permissions" in this manual

In this manual, *Administrator permissions* refers to the Administrator permissions for the local PC. Provided that the user has Administrator permissions for the local PC, operations are the same whether they are performed with a local user account, a domain user account, or in an Active Directory environment.

■ 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*.

■ Conventions: Paths specified in definition files

A definition cannot include any file name that is specified with a network path.

For example, the event guide information file must have `EV_FILE` specified with a folder path that is not a network path.

■ Online manuals

JP1/IM comes with an HTML manual that you can read in a web browser.

The HTML manual has the same contents as this manual.

To view the HTML manual:

- In JP1/IM - View, choose **Help** and then **Help Contents**.
- In Integrated Operation Viewer Window, choose **Help** and then **Online manual**.

Note:

- If you use the **Start** menu, the HTML manual may be displayed in an existing browser window, depending on the related setting in the OS.

■ Output destinations of Integrated trace log file

Starting with JP1/IM 12-10, all 32-bit Java processes for JP1/IM have been changed to 64-bit Java processes. Therefore, the integrated trace log output destination output by the Java process function of each function of JP1 / IM is changed.

The following is the destination of the integrated trace log for each JP1/IM function from version 12-10 or later. If you are using the log file trap function, you must change the settings as you change the destination.

Output destinations of Integrated trace log file (32 bit): *system-drive*`\Program Files(x86)\Hitachi\HNTRLib2\spool`

- IM database
- Central Scope Service
- Process management

- Command execution
- Automatic action
- Installation and Setup

Output destinations of Integrated trace log file (64 bit): *system-drive*`\Program Files\Hitachi\HNTRLib2\spool`

- Event base service
- Central Console viewer
- Central Scope viewer
- Event Genaration Service
- IM Configuration Management
- IM Configuration Management viewer
- Intelligent Integrated Management Base

Contents

1 Commands

This chapter describes the syntax of the commands that are used in JP1/IM.

Format of command explanations

This section describes the format of the command explanations. Note that some of the items shown below might be omitted in some command explanations.

Function

Describes the function of the command.

Format

Describes the command's format.

Execution permission

Describes the user permissions required in order to execute the command.

Storage directory

Describes the command's storage location.

Arguments

Describes the arguments of the command.

Note that arguments are case sensitive (except for the `ON` and `OFF` arguments, which are not case sensitive).

The jpc_service command and the jpc_service_autostart command `-on` and `-off` are case-sensitive.

Notes

Provides additional important information about the command.

Return values

Describes the command's return values.

For details about the messages that may be displayed during command execution, see the *JP1/Integrated Management 3 - Manager Messages*.

Example

Provides an example of using the command.

Example output

Provides an example of the output from execution of the command.

Lists of commands

This section lists the names of the commands that can be used in JP1/IM and the permissions required to execute these commands. Note that the commands are described in alphabetical order from the next section.

Legend and notes for tables

Whether a command is supported in the Windows and UNIX environments is indicated in the tables by the following notations and notes:

Legend:

Y: Supported

--: Not supported

#1

In Windows, a superuser means a user with Administrator permissions.

#2

This is a JP1/Base command (related to configuration definition and command execution) for the manager. For details about the command, see the chapter that describes commands in the *JP1/Base User's Guide*.

#3

In Windows, Administrator permissions are required. (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

#4

This command is used by the monitored AIX host.

Commands related to startup, termination, and setup

Overview of function	Command name	Windows	UNIX	Required execution permission
Sets up JP1/IM - Manager (Central Console)	*jp1cc_setup (UNIX only)*	--	Y	Superuser
Sets up JP1/IM - Manager (Central Scope)	*jp1cs_setup (UNIX only)*	--	Y	Superuser
Starts JP1/IM - Manager automatically	*jco_start (UNIX only)*	--	Y	Superuser
Terminates JP1/IM - Manager automatically	*jco_stop (UNIX only)*	--	Y	Superuser
Displays the status of JP1/IM - Manager processes	*jco_spmd_status*	Y	Y	Superuser#1
Updates the status of JP1/IM - Manager processes	*jco_spmd_reload*	Y	Y	Superuser#1
Specifies settings required for operation in a cluster system	*jp1cohasetup (Windows only)*	Y	--	Superuser#1
	jp1cshasetup (Windows only)	Y	--	Superuser#1
	jp1cc_setup_cluster (UNIX only)	--	Y	Superuser
	jp1cs_setup_cluster (UNIX only)	--	Y	Superuser
Starts JP1/IM - Manager in a cluster system	*jco_start.cluster (UNIX only)*	--	Y	Superuser

Overview of function	Command name	Windows	UNIX	Required execution permission
Terminates JP1/IM - Manager in a cluster system	*jco_stop.cluster (UNIX only)*	--	Y	Superuser
Forcibly terminates JP1/IM - Manager in a cluster system	*jco_killall.cluster (UNIX only)*	--	Y	Superuser
Specifies dependencies between JP1/IM-Manager Service and the JP1/Base Event service	*SpmSetSvcCon (Windows only)*	Y	--	Superuser[#1]

Commands related to IM databases

Overview of function	Command name	Windows	UNIX	Required execution permission
Sets up the IM Configuration Management database for storing configuration information	*jcfdbsetup*	Y	Y	Superuser[#1]
Cancels setup of the IM Configuration Management database that stores configuration information	*jcfdbunsetup*	Y	Y	Superuser[#1]
Sets up an integrated monitoring database for storing JP1 events	*jcodbsetup*	Y	Y	Superuser[#1]
Cancels setup of the integrated monitoring database that stores JP1 events	*jcodbunsetup*	Y	Y	Superuser[#1]
Outputs to a CSV file JP1 event information registered in the integrated monitoring database	*jcoevtreport*	Y	Y	Superuser[#1]
Backs up the IM database	*jimdbbackup*	Y	Y	Superuser[#1]
Releases free area (free page area) in the IM Configuration Management database	*jimdbreclaim*	Y	Y	Superuser[#1]
Restores (recovers) a database from a backup that has been stored	*jimdbrecovery*	Y	Y	Superuser[#1]
Reorganizes fragmented free space in a database	*jimdbrorg*	Y	Y	Superuser[#1]
Checks the operating status of the IM database (such as running or stopped)	*jimdbstatus*	Y	Y	Superuser[#1]
Terminates the IM database	*jimdbstop*	Y	Y	Superuser[#1]
Updates the IM database	*jimdbupdate*	Y	Y	Superuser[#1]

Commands related to IM Configuration Management

Overview of function	Command name	Windows	UNIX	Required execution permission
Collects virtualization configuration information from HCSM, and outputs it to the virtualization configuration information file	*jcfcolvmhcsm*	Y	Y	Superuser[#1]
Collects virtualization configuration information from KVM, and outputs it to the virtualization configuration information file	*jcfcolvmkvm*	Y	Y	Superuser[#1]

Overview of function	Command name	Windows	UNIX	Required execution permission
Collects virtualization configuration information from SCVMM, and outputs it to the virtualization configuration information file	*jcfcolvmscvmm (Windows only)*	Y	--	Superuser[#1]
Collects virtualization configuration information from vCenter, and outputs it to the virtualization configuration information file	*jcfcolvmvc*	Y	Y	Superuser[#1]
Collects virtualization configuration information from Hitachi Compute Blade logical partitioning feature, and outputs it to the virtualization configuration information file	*jcfcolvmvirtage*	Y	Y	Superuser[#1]
Acquires virtualization configuration information from VMware ESX and outputs it to a virtualization configuration information file	*jcfcolvmesx*	Y	Y	Superuser[#1]
Outputs the hierarchical configuration (IM configuration) of a system managed by IM Configuration Management, host information, and definition information	*jcfexport*	Y	Y	Superuser[#1]
Imports IM Configuration Management information	*jcfimport*	Y	Y	Superuser[#1]
Creates from the host input information file and Central Scope export file a Central Scope import file that contains monitoring tree information for a virtualization configuration. Alternatively, creates from the business group information file, monitoring group information file, and Central Scope export file a Central Scope import file to which the monitoring tree information of a business group has been added	*jcfmkcsdata*	Y	Y	Superuser[#1]
Uses a virtualization configuration information file to update a host input information file	*jcfmkhostsdata*	Y	Y	Superuser[#1]
Updates the virtualization configuration of the specified host	*jcfvirtualchstat*	Y	Y	Superuser[#1]
Sets up an operating environment for the IM Configuration Management processes of JP1/IM - Manager	*jp1cf_setup (UNIX only)*	--	Y	Superuser
Sets up an environment for IM Configuration Management for cluster system operation	*jp1cf_setup_cluster (UNIX only)*	--	Y	Superuser
Sets up an environment for IM Configuration Management for cluster system operation	*jp1cfhasetup (Windows only)*	Y	--	Superuser[#1]

Commands related to IM Configuration Management (remote monitoring configuration)

Overview of function	Command name	Windows	UNIX	Required execution permission
Defines the profile of a remote monitoring event log trap on the specified monitored host	*jcfaleltdef (Windows only)*	Y	--	Superuser[#1]
Reloads a remote monitoring event log trap action definition file	*jcfaleltreload (Windows only)*	Y	--	Superuser[#1]

Overview of function	Command name	Windows	UNIX	Required execution permission
Starts a remote monitoring event log trap	*jcfaleltstart (Windows only)*	Y	--	Superuser#1
Displays the operating status of a remote monitoring event log trap	*jcfaleltstat (Windows only)*	Y	--	Superuser#1
Stops a remote monitoring event log trap	*jcfaleltstop (Windows only)*	Y	--	Superuser#1
Adds or deletes the profile of a remote monitoring log file trap on the specified monitored host	*jcfallogdef*	Y	Y	Superuser#1
Reloads the action definition file of a remote monitoring log file trap	*jcfallogreload*	Y	Y	Superuser#1
Starts a remote monitoring log file trap	*jcfallogstart*	Y	Y	Superuser#1
Displays the operating status of a remote monitoring log file trap	*jcfallogstat*	Y	Y	Superuser#1
Stops a remote monitoring log file trap	*jcfallogstop*	Y	Y	Superuser#1

Commands related to upgrading

Overview of function	Command name	Windows	UNIX	Required execution permission
Converts an action definition file from version earlier than 11-50 to version 11-50 or later	*jcadefconv*	Y	Y	Superuser#1
Changes the location of the event acquisition filter from Event Console Service to Event Base Service (when the event acquisition filter is being used for compatibility)	*jcochafmode (UNIX only)*	Y	Y	Superuser#1
Migrates JP1/Base command execution logs for version 7 or earlier to a command execution log file for version 8	`jcocmdconv`#2	Y	Y	Superuser#1
Upgrades a logical host environment that was set up using a previous version of JP1/IM - Manager or JP1/IM - Manager (Central Console)	*jp1cohaverup*	Y	Y	Superuser#1
Upgrades a physical host environment from a previous version of JP1/IM - Manager (Central Scope)	*jp1csverup.bat (Windows only)*	Y	--	Superuser#1
Upgrades a logical host environment that was set up using a previous version of JP1/IM - Manager (Central Scope)	*jp1cshaverup.bat (Windows only)*	Y	--	Superuser#1
Upgrades a physical host environment from a previous version of JP1/IM - Manager (Central Scope)	*jp1csverup (UNIX only)*	--	Y	Superuser
Upgrades a logical host environment that was set up using a previous version of JP1/IM - Manager (Central Scope)	*jp1cshaverup (UNIX only)*	--	Y	Superuser

Commands related to the Intelligent Integrated Management Base

Overview of function	Command name	Windows	UNIX	Required execution permission
Collects the configuration information of the system managed by JP1/IM - Manager (Intelligent Integrated Management Base) and creates the IM management node-related files	*jddcreatetree*	Y	Y	Superuser[#1]
Collects system configuration information from the products managed by the Intelligent Integrated Management server, and creates IM management node-related files that are used as input data for the `jddupdatetree` command	*jddupdatetree*	Y	Y	Superuser[#1]
Sets a user ID and password that are used for JP1/IM - Manager (Intelligent Integrated Management Base) to be authenticated by linked products	*jddsetaccessuser*	Y	Y	Superuser[#1]
Sets authentication information for the proxy server when REST APIs are executed from plug-ins that are provided by JP1/IM - Manager (Intelligent Integrated Management Base)	*jddsetproxyuser*	Y	Y	Superuser[#1]
Loads user-defined suggestion definition files and applies them to JP1/IM - Manager (Intelligent Integrated Management Base).	*jddupdatesuggestion*	Y	Y	Superuser[#1]
Takes the Intelligent Integrated Management Base client information registered with the OpenID provider for OpenID authentication linkage, and sets it in JP1/IM - Manager (Intelligent Integrated Management Base).	*jddsetopinfo*	Y	Y	Superuser[#1]
Takes the mapping information defined in the single sign-on mapping definition file and applies it to JP1/IM - Manager (Intelligent Integrated Management Base).	*jddupdatessomap*	Y	Y	Superuser[#1]
Import the user-defined automatic action definition file and reflect it in the intelligent integrated management infrastructure.	*jddupdateaction*	Y	Y	Superuser[#1]

Commands related to the Intelligent Integrated Management Database

Overview of function	Command name	Windows	UNIX	Required execution permission
Backup the Intelligent Integrated Management Database.	*jimgndbbackup*	Y	Y	Superuser[#1]
Recover the Intelligent Integrated Management Database stored in backup.	*jimgndbrestore*	Y	Y	Superuser[#1]
Setup the Intelligent Integrated Management Database and the Trend Data Management Service.	*jimgndbsetup*	Y	Y	Superuser[#1]
Un-setup the Intelligent Integrated Management Database and the Trend Data Management Service.	*jimgndbunsetup*	Y	Y	Superuser[#1]
Stop the Intelligent Integrated Management Database Service and the Trend Data Management Service.	*jimgndbstop*	Y	Y	Superuser[#1]
Checking the operating status of the Intelligent Integrated Management Database Service and the Trend Data Management Service.	*jimgndbstatus*	Y	Y	Superuser[#1]

■About multiple execution of the commands related to the Intelligent Integrated Management Database

The following table shows possible or not possible multiple execution of the commands related to the Intelligent Integrated Management Database.

<table>
<tr><th rowspan="2">Execute command name</th><th colspan="6">Executing command name</th></tr>
<tr><th>jimgndbsetup</th><th>jimgndbunsetup</th><th>jimgndbstop</th><th>jimgndbstatus</th><th>jimgndbbackup</th><th>jimgndbrestore</th></tr>
<tr><td>jimgndbsetup</td><td colspan="3">Not possible</td><td>Possible</td><td colspan="2">Not possible</td></tr>
<tr><td>jimgndbunsetup</td><td colspan="3">Not possible</td><td>Possible</td><td colspan="2">Not possible</td></tr>
<tr><td>jimgndbstop</td><td colspan="3">Not possible</td><td>Possible</td><td colspan="2">Not possible</td></tr>
<tr><td>jimgndbstatus</td><td colspan="6">Possible</td></tr>
<tr><td>jimgndbbackup</td><td colspan="3">Not possible</td><td>Possible</td><td colspan="2">Not possible</td></tr>
<tr><td>jimgndbrestore</td><td colspan="3">Not possible</td><td>Possible</td><td colspan="2">Not possible</td></tr>
</table>

Commands related to views

Overview of function	Command name	Windows	UNIX	Required execution permission
Starts IM Configuration Management - View	*jcfview (Windows only)*	Y	--	None
Registers into or deletes from the Windows **Start** menu the menu item for starting IM Configuration Management - View	*jcovcfsetup (Windows only)*	Y	--	Superuser[#1]
Opens JP1/IM - View's Login window or Monitoring Tree (Editing) window, or logs in to JP1/IM - Manager from the command line	*jcoview (Windows only)*	Y	--	None

Commands related to configuration definition

Overview of function	Command name	Windows	UNIX	Required execution permission
Distributes configuration definition information to the lower hosts and enables the definition information	jbsrt_distrib[#2]	Y	Y	Superuser[#1]
Collects configuration definition information from the lower hosts and updates the configuration definition	jbsrt_sync[#2]	Y	Y	Superuser[#1]
Deletes the configuration definition information for the host that executed the command	jbsrt_del[#2]	Y	Y	Superuser[#1]
Displays the existing configuration definition information	jbsrt_get[#2]	Y	Y	Superuser[#1]

Commands related to events

Overview of function	Command name	Windows	UNIX	Required execution permission
Changes the response status for severe events	*jcochstat*	Y	Y	None[#3]

Overview of function	Command name	Windows	UNIX	Required execution permission
Sets up a JP1/IM - Manager system environment	*jcoimdef*	Y	Y	Superuser[#1]

Commands related to automated actions and command execution

Overview of function	Command name	Windows	UNIX	Required execution permission
Checks the definitions of automated actions and merges multiple automated action definition files	*jcamakea*	Y	Y	Superuser[#1]
Displays the result of automated action execution	*jcashowa*	Y	Y	None[#3]
Displays to standard output the status of the Automatic Action Service that is running and the contents of the automated action definition file that is loaded.	*jcastatus*	Y	Y	None[#3]
Reloads the automated action definitions, places the automated action function on standby, or enables or disables the automated action definition.	*jcachange*	Y	Y	Superuser[#1]
Cancels automated actions	*jcacancel*	Y	Y	Superuser[#1]
Sets up a command execution environment	`jcocmddef`[#2]	Y	Y	Superuser[#1]
Outputs logs of executed commands	`jcocmdlog`[#2]	Y	Y	None
Deletes commands that were executed from JP1/IM - View or executed by automated actions	`jcocmddel`[#2]	Y	Y	Superuser[#1]
Checks the status of commands that were executed from JP1/IM - View or executed by automated actions	`jcocmdshow`[#2]	Y	Y	Superuser[#1]

Commands related to the email notification function

Overview of function	Command name	Windows	UNIX	Required execution permission
Sends email to the specified email address	*jimmail (Windows only)*	Y	--	Superuser[#1]
Sets the password for POP before SMTP authentication or SMTP-AUTH authentication in the email environment definition file	*jimmailpasswd (Windows only)*	Y	--	Superuser[#1]

Commands related to correlation event generation

Overview of function	Command name	Windows	UNIX	Required execution permission
Changes correlation event generation definitions	*jcoegschange*	Y	Y	Superuser[#1]
Checks the contents of a correlation event generation definition file	*jcoegscheck*	Y	Y	Superuser[#1]

Overview of function	Command name	Windows	UNIX	Required execution permission
Places the correlation event generation function in correlation running status	*jcoegsstart*	Y	Y	Superuser[#1]
Displays the status of the correlation event generation function and the correlation event generation definitions that are being used currently	*jcoegsstatus*	Y	Y	None[#3]
Places the correlation event generation function in standby status	*jcoegsstop*	Y	Y	Superuser[#1]

Commands used in the Central Scope environment setup

Overview of function	Command name	Windows	UNIX	Required execution permission
Registers host information into the host information database	*jcshostsimport*	Y	Y	Superuser[#1]
Acquires host information from the host information database	*jcshostsexport*	Y	Y	Superuser[#1]
Creates or re-creates the monitoring object database	*jcsdbsetup*	Y	Y	Superuser[#1]

Commands related to filters

Overview of function	Command name	Windows	UNIX	Required execution permission
Switches the event acquisition filter	*jcochfilter*	Y	Y	Superuser[#1]
Changes the operating mode of the common exclusion-conditions	*jcochcefmode*	Y	Y	Superuser[#1]

Commands related to changing the monitoring node status in Central Scope

Overview of function	Command name	Windows	UNIX	Required execution permission
Changes the status of monitoring nodes (monitoring objects or monitoring groups)	*jcschstat*	Y	Y	Superuser[#1]

Commands for migrating monitoring object database information in Central Scope

Overview of function	Command name	Windows	UNIX	Required execution permission
Acquires monitoring object database storage information from JP1/IM - Manager and outputs it locally to a file	*jcsdbexport*	Y	Y	Superuser[#1]
Applies the information output to a file by the `jcsdbexport` command to the monitoring object database of JP1/IM - Manager	*jcsdbimport*	Y	Y	Superuser[#1]

Commands used for troubleshooting

Overview of function	Command name	Windows	UNIX	Required execution permission
Creates a Java thread dump of IM Configuration Management - View	*jcfthreaddmp (Windows only)*	Y	--	None
Collects data in the event of a failure in JP1/IM - Manager or JP1/IM - View	*jim_log.bat (Windows only)*	Y	--	None#3
Collects data in the event of a failure in JP1/IM - Manager	*jim_log.sh (UNIX only)*	--	Y	Superuser
Collects data in the event of a failure in JP1/IM - View	*jcoview_log.bat (Windows only)*	Y	--	None#3
Outputs a thread dump in the event of a failure in JP1/IM - View	*jcothreaddmp (Windows only)*	Y	--	None
Outputs a thread dump and a core dump (UNIX only) in the event of a failure in JP1/IM - Manager	*jcogencore*	Y	Y	Superuser#1
Tests the notification command that is defined in the health check definition file in JP1/IM - Manager	*jcohctest*	Y	Y	Superuser#1

Commands for checking the contents of the JP1/IM - Manager definition file

Overview of function	Command name	Windows	UNIX	Required execution permission
Checks the definition file for extended event attributes	*jcoattrfcheck*	Y	Y	None#3
Checks the definition file for opening monitor windows	*jcomonitorfcheck*	Y	Y	None#3

Commands for checking the contents of the JP1/IM - View definition file

Overview of function	Command name	Windows	UNIX	Required execution permission
Checks the definition file for executing applications	*jcoappexecfcheck (Windows only)*	Y	N	None
Checks the definition file for the Tool Launcher window	*jcofuncfcheck (Windows only)*	Y	N	None

Command that counts the number of nodes managed by JP1/IM - Manager

Overview of function	Command name	Windows	UNIX	Required execution permission
Counts the number of nodes managed by JP1/IM - Manager	*jimnodecount*	Y	Y	Superuser#1

Commands related to the JP1/IM - Agent

Overview of function	Command name	Windows	UNIX	Required execution permission
Perform configuration file format checks and test alert rules for Prometheus server	*promtool*	Y	Y	None
Obfuscate the specified secret and store it in the secret manager File	*jimasecret*	Y	Y	Superuser[#1]
Perform an early Setup of JP1/IM - Agent	*jimasetup*	Y	Y	Superuser[#1]
Setup enable or disable of add-on program of JP1/IM - Agent.	*jpc_service*	Y	Y	Superuser[#1, #3]
Setup JP1/IM - Agent to start and stop automatically	*jpc_service_autostart*	Y	Y	Superuser[#1, #3]
Start JP1/IM - Agent Services	*jpc_service_start*	Y	Y	Superuser[#1, #3]
Stop JP1/IM - Agent Services	*jpc_service_stop*	Y	Y	Superuser[#1, #3]
Shut down Node exporter for AIX	*jpc_stop_node_exporter_aix (AIX only)*	--[#4]		Superuser

Commands for SAP system monitoring

Overview of function	Command name	Windows	UNIX	Required execution permission
Extracts the system log information of the SAP system.	*jr3slget*	Y	Y	None
Extracts the CCMS alert information of the SAP system.	*jr3alget*	Y	Y	None

Notes common to all commands

Notes about 32-bit cmd.exe(for Windows)

These commands are not compatible for 32-bit cmd.exe. Use 64-bit cmd.exe instead.

Notes about parallel execution

The following commands or functions are not allowed to run in parallel.

- jpc_service
- jpc_service_autostart
- jpc_service_start
- jpc_service_stop
- definition file manipulation function

Notes about the environment without systemd(for Linux)

The following commands or functions are not allowed to run in the environment without systemd(e.g. container environments).

- jpc_service
- jpc_service_autostart
- jpc_service_start
- jpc_service_stop
- definition file manipulation function(uploading JP1/IM - Agent definition files)

jcacancel

Function

This command cancels automated actions. It is used to delete from JP1/IM - Manager the following actions that are no longer needed for system operation:

- Actions that remain in the queuing state without being executed because many automated actions have been performed during system operation
- Actions that remain in the running state because a command that needs time to be processed or processing of which does not end has been executed

The command executed for an action can be deleted by the `jcocmddel` command, but the status of the action does not change to canceled. Use the `jcocmddel` command to delete an action that cannot be canceled by using the `jcacancel` command.

For details about the `jcocmddel` command, see the chapters related to commands in the *JP1/Base User's Guide*.

The action status after cancellation depends on the action status before cancellation. The following table lists and describes the action statuses that can be canceled and the action statuses after cancellation.

Table 1–1: Statuses of actions that can be canceled and the action statuses after cancellation

Status of action that can be canceled	Action status after cancellation[#1]
`Wait` or `Wait (Miss)`	`Cancel`
`Send (Miss)`[#2]	
`Queue` or `Queue (Miss)`	
`Running` or `Running (Miss)`	`Kill`

#1: If an error occurs in JP1/Base command control during cancellation processing, the action status is set to `Error (Miss)`.

#2: An action whose status is `Send` cannot be canceled. If an attempt is made to cancel such an action, the action status is set to `Send (Miss)`.

Format

```
jcacancel [-h logical-host-name]
          {[-i action-serial-number,...] | [-a] | [-s action-executing-host
-name]}
          [-f]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command cancels automated actions that correspond to the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-i` *action-serial-number*

Specifies an automated action that is to be canceled.

You can determine the action serial numbers by using the `jcashowa` command or by displaying the List of Action Results window and the Action Log Details window in JP1/IM - View. You can specify a maximum of 20 action serial numbers. If you specify multiple action serial numbers, separate them with the comma (`,`). No other options can be specified between action serial numbers.

If you specify multiple action serial numbers and an error occurs on one action serial number during execution, processing continues. As many error messages are displayed as there are errors.

If you specify multiple action serial numbers in the `-i` option (in order to cancel multiple actions) and then multiple errors occur, the return value of the `jcacancel` command is for the last error that occurred.

`-a`

Specifies that all automated actions that are to be executed from the JP1/IM where `jcacancel` is executed and that exist on all monitored hosts are to be canceled.

If you specify the `-a` option to cancel multiple actions and multiple errors occur, the return value of the `jcacancel` command is for the last error that occurred.

`-s` *action-executing-host-name*

Specifies a host name when the automated actions that are to be canceled are the automatic actions executed from the JP1/IM where `jcacancel` is executed and that exist on the specified action executing host.

You can specify only a host that has been set as a managed host in the system configuration definition. Neither an IP address nor a host group can be specified.

If you specify the `-s` option to cancel multiple actions and multiple errors occur, the return value of the `jcacancel` command is for the last error that occurred.

`-f`

Specifies that the automated actions are to be canceled without displaying a configuration message during cancellation processing.

Notes

- Processing if the target host is restarted during cancellation processing

  If the target host where automated actions are to be executed is restarted during automated action cancellation processing, the cancellation status of actions cannot be acquired. Therefore, the action status remains as `Wait (Canceling)`, `Send (Canceling)`, `Queue (Canceling)`, or `Running (Canceling)`, making it impossible to determine whether cancellation processing was successful. Use the `jcocmdshow` command to check the results. If there are any remaining actions, delete them with the `jcocmddel` command.

Return values

0	Normal termination
1	Invalid argument error
2	Invalid common definition error
3	Invalid action status error
4	Cancellation processing error
5	Input/output error
6	There was no response from the automated action function (Automatic Action Service)
7	Execution permission error (Windows only)
255	System error

Example 1

Cancel multiple automated actions (action serial numbers 23, 35, and 42):

```
jcacancel -i 23,35,42
```

Example 2

Cancel all automated actions that are executed from the hostA logical host and that exist on all hosts that are monitored by the hostA logical host:

```
jcacancel -h hostA -a
```

Example 3

Cancel the automated actions that are executed from the JP1/IM that executes jcacancel and that exist on the host01 host:

```
jcacancel -s host01
```

Example 4

Cancel the automated actions that are executed from the hostB logical host and that exist on host02, which is monitored by the hostB logical host:

```
jcacancel -h hostB -s host02
```

Example 5

Cancel the automated actions that are monitored by the hostC logical host and that have specified action serial numbers (23, 35, and 42):

```
jcacancel -h hostC -i 23,35,42
```

jcachange

Function

This command reloads the automated action definition file, places the automated action function on standby, or, enables or disables the automated action definition.

If both options are omitted, the command reloads the automated action definition file. After you have changed the contents of the automated action definition file, you use this command to activate the modified action definitions by reloading the file.

This command skips invalid action definitions in the automated action definition file, and continues processing.

If the automated action definition file contains an invalid action definition, the command displays the `KAVB5104-W` message. If you want to reload the automated action definition file you edited, before executing the `jcachange` command, execute the `jcamakea` command to make sure that there are no errors in the automated action definition file.

If the `KAVB5104-W` message is displayed, review the contents of the automated action definition file.

If the loaded automated action definition file contains no valid action definitions, the command displays the `KAVB4053-I` message and places the automated action function on standby.

When this command is executed with no option specified, the suppression time and the status of satisfied AND-joined conditions are initialized for all action execution conditions. When this command is executed with the `-e`, `-on`, `-off`, or `-st` option specified, the suppression time and the status of satisfied AND-joined conditions are not initialized unless the definition of the action execution condition is changed.

A reloaded automated action definition parameter that exceeds the maximum size is ignored by the command. For details about the size of an automated action definition parameter, see *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files*.

Format

```
jcachange [-n] [-h logical-host-name]
          [-e [action-ID[,action-ID...] | ALL]]
          [-on action-ID[,action-ID...]]
          [-off action-ID[,action-ID...]]
          [-st]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-n`

Specifies that the automated action function is to be placed on standby. No actions are executed even if an event that matches an action definition is received.

To restart the automated action function, either execute the `jcachange` command with no options specified or restart JP1/IM - Manager.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command reloads or places on standby the action definitions for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-e [`*action-ID*`[,`*action-ID*`...] | ALL]`

Specifies the action ID of an action definition to enable. Other action definitions whose IDs are not specified in this option are disabled. To specify multiple IDs, separate them with a comma (`,`). To enable all actions, specify `ALL`.

Executing the command with this option changes every `valid` parameter in the action definition file. When the action ID is specified, the corresponding `valid` parameter is changed to `true`. When the action ID is not specified, it is changed to `false`. When `ALL` is specified, all `valid` parameters are changed to `true`.

This option is available only when `DESC_VERSION` of the action definition file is `4`.

When the action definition of a specified action ID is not found in the action definition file, the `KAVB4028-E` message is sent to the standard error output and integrated trace log, and the command ends with a return code of `10`. When no action execution condition is defined in the action definition file and `ALL` is specified for this option, the `KAVB4029-E` message is sent to the standard error output and integrated trace log, and the command ends with a return code of `10`. When no action execution condition is defined in the action definition file and no action ID is specified for this option, the `KAVB4029-E` message is sent to the standard error output and integrated trace log, and the command ends with a return code of `11`.

`-on` *action-ID*`[,`*action-ID*`...]`

Specifies the action ID of an action definition to enable. To specify multiple IDs, separate them with a comma (`,`). The status of other action definitions whose IDs are not specified remains the same. This option cannot be combined with the `-e` option.

Executing the command with this option changes the `valid` parameters of the specified action IDs in the action definition file to `true`.

This option is available only when `DESC_VERSION` of the action definition file is `4`.

When the action definition of a specified action ID is not found in the action definition file, the `KAVB4028-E` message is sent to the standard error output and integrated trace log, and the command ends with a return code of `10`.

`-off` *action-ID*`[,`*action-ID*`...]`

Specifies the action ID of an action definition to disable. To specify multiple IDs, separate them with a comma (`,`). The status of other action definitions whose IDs are not specified remains the same. This option cannot be combined with the `-e` option.

Executing the command with this option changes the `valid` parameters of the specified action IDs in the action definition file to `false`.

This option is available only when `DESC_VERSION` of the action definition file is `4`.

When the action definition of a specified action ID is not found in the action definition file, the `KAVB4028-E` message is sent to the standard error output and integrated trace log, and the command ends with a return code of `11`.

`-st`

Specifies that executing the command will not initialize the suppression status and the status of satisfied conditions of the AND-joined conditions when the following is true for the action execution condition:

- There is no difference between the definition of the action execution condition that works in the Event Base Service and the definition that is specified in the action definition file.

This option is available only when `DESC_VERSION` of the action definition file is `4`. Only the `-h` option can be combined with this option.

Notes

Executing the `jcachange` command concurrently many times might cause timeouts or a degraded performance of managers.

Return values

`0`	Normal termination
`4`	There was no response from the automated action function
`5`	Command failed to reload the automated action definition file or place the automated action function on standby
`10`	There is no action definition that is to be enabled
`11`	There is no action definition that is to be disabled
`12`	Failed to update due to failure to acquire exclusive rights for the automated action definition file
`13`	Failed to read due to failure to acquire exclusive rights for the automated action definition file
`111`	Failed to connect to the Event Base Service or the Event Console Service (in UNIX)
`154`	File input/output error (in UNIX)
`243`	A specified argument value was invalid (in UNIX)
`-13`	A specified argument value was invalid (in Windows)
`-102`	File input/output error (in Windows)
`-401`	Failed to connect to the Event Base Service or the Event Console Service (in Windows)
Other value	System error

jcadefconv

Function

This command converts an action definition file from version earlier than 11-50 (`DESC_VERSION` value is less than 4) to version 11-50 or later (`DESC_VERSION` value is 4).

If the action definition file for version 8 or earlier uses any of the characters listed below in its messages or in basic event information, detailed event information, or extended event information, the file is converted and defined.

Table 1–2: Character conversion

Character before conversion	Characters after conversion
\/	/
Space	%20
%	%25

Before it executes this conversion, this command automatically checks the format of the action definition file. If it detects any errors, the action definition file is not converted and the command outputs error messages to standard error.

You can specify any output destination for the converted action definition file.

An action definition file is converted from version 8 or earlier to version 11-50 or later as shown below.

Table 1–3: Conversion of action definition files

Format of version 8 or earlier	Format of version 11-50 or later	Remarks
No `DESC_VERSION`	`DESC_VERSION=4`	--
`DESC_VERSION=1`	`DESC_VERSION=4`	--
`DESC_VERSION=2`	`DESC_VERSION=4`	--
`DESC_VERSION=3`	`DESC_VERSION=4`	--

`:state_watch=true`	`cmn`
	▲ `staΔtrue`
	`end-cmn`
		--

`:state_watch=false`	`cmn`
	▲ `staΔfalse`
	`end-cmn`
		--

`:state_watch` not specified	`cmn`
	▲ `staΔfalse`
	`end-cmn`
		--

#*comment-1*
`+0Δ*Δ:action.exe`
	`actΔ`*action-1*
	▲ `prmΔ0`
	▲ `cmtΔ`*comment-1*
	`...`
	`end-act`
		--

#Δ*comment-1* `+0Δ*Δ:action.exe`	`actΔ`*action-1* ▲ `prmΔ0` ▲ `cmt` ▲▲ *comment-1*	--

Format of version 8 or earlier	Format of version 11-50 or later	Remarks
	... end-act	
#*comment-1* #*comment-2* +0Δ*Δ:action.exe	actΔ*action-1* ▲ prmΔ0 ▲ cmtΔ*comment-2* ... end-act	--
Action specifying a parameter group	actΔ*action-serial-number*	When the command is executed in an Japanese language environment
	actΔ*action-serial-number*	When the command is executed in an English language environment
AND action	act	--
+*parameter-group-number*	▲ prmΔ*parameter-group-number*	--
&	▲ prmΔ&	--
$*basic-part-of-event-ID*	▲ eidΔ*basic-part-of-event-ID*	--
$*basic-part-of-event-ID*:*extended-part-of-event-ID*	▲ eidΔ*basic-part-of-event-ID*:*extended-part-of-event-ID*	--
*	▲ eidΔ*	--
/*message*/	▲▲ B.MESSAGEΔREGEXΔ*message*	--
/*basic-event-information*/	▲▲ B.BASICΔREGEXΔ*basic-event-information*	--
/*detailed-event-information*/	▲▲ B.DETAILΔREGEXΔ*detailed-event-information*	--
//	No condition is set	--
/-------E/	▲▲ E.SEVERITYΔINΔEmergency	--
/------A-/	▲▲ E.SEVERITYΔINΔAlert	--
/-----C--/	▲▲ E.SEVERITYΔINΔCritical	--
/----E---/	▲▲ E.SEVERITYΔINΔError	--
/---W----/	▲▲ E.SEVERITYΔINΔWarning	--
/--N-----/	▲▲ E.SEVERITYΔINΔNotice	--
/-I------/	▲▲ E.SEVERITYΔINΔInformation	--
/D-------/	▲▲ E.SEVERITYΔINΔDebug	--
/DINWECAE/	▲▲ E.SEVERITYΔINΔEmergencyΔAlertΔCriticalΔErrorΔWarningΔNoticeΔInformationΔDebug	When a condition with multiple event levels is specified
extended-event-information-attribute-name=/*attribute-value*/	▲▲ E.*extended-event-information-attribute-name*ΔREGEXΔ*attribute-value*	--
u=*user-name*	▲ usrΔ*user-name*	--
e=*environment-variable-file-name*	▲ varΔ*environment-variable-file-name*	--
d=*execution-host-name*	▲ hstΔ*execution-host-name*	--

Format of version 8 or earlier	Format of version 11-50 or later	Remarks
`d=`*group-name*	▲`hst`Δ*group-name*	--
`dt=`*suppression-time*	▲`det`Δ*suppression-time*	--
`rt=`*delay-monitoring-period*	▲`ret`Δ*delay-monitoring-period*	--
`+0`Δ`*`Δ`:`*action*	▲`cmd`Δ*action*	--
`+0`Δ`*`Δ`:<RULE>`	▲`rule`	When JP1/IM - RL is executed
`+0`Δ`*`Δ`:action.exe`	`act`Δ*action-1* ▲`prm`Δ`0` ▲`eid`Δ`*` ▲`cnd` ▲`end-cnd` ▲`cmd`Δ`action.exe` `end-act`	When there is no event condition
`+0`Δ`*`Δ`/`*message*`/ : action.exe`	`act`Δ*action-1* ▲`prm`Δ`0` ▲`eid`Δ`*` ▲`cnd` ▲▲`B.MESSAGE`Δ`REGEX`Δ*message* ▲`end-cnd` ▲`cmd`Δ`action.exe` `end-act`	When there is an event condition
--	`aid`Δ *action-ID*	An action ID is assigned to an action execution condition from the top of the action definition in the order at which the action execution conditions are listed. The ID increments from 0 to 2,147,483,647. Note that no action ID is assigned to the action execution condition whose parameter group is set to `&`.
--	`valid`Δ`true`	The `valid` parameter is set to `true` (enabled). However, this parameter is not changed for the action execution condition whose parameter group is set to `&`.

Legend:

▲ : Indicates a tab

Δ: Indicates a space

--: None

Format

```
jcadefconv -i action-definition-file-name-before-conversion
           -o action-definition-file-name-after-conversion
          [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-i` *action-definition-file-name-before-conversion*

Specifies the relative or absolute path name of the action definition file that is to be converted. If the path name of the action definition file contains a space, enclose the entire path name in double quotation marks (`"`). The file name can consist of a maximum of 255 bytes.

`-o` *action-definition-file-name-after-conversion*

Specifies the relative or absolute path name of the action definition file that is obtained after conversion. If the path name of the action definition file contains a space, enclose the entire path name in double quotation marks (`"`). The file name can consist of a maximum of 255 bytes.

Note that the following characters and character strings cannot be specified in a file name in Windows:

- Characters: `:` `?` `"` `<` `>` `|`
- A character string that completely matches any of the following strings (not case sensitive): `CON`, `PRN`, `AUX`, `NUL`, `COM1`, `COM2`, `COM3`, `COM4`, `COM5`, `COM6`, `COM7`, `COM8`, `COM9`, `LPT1`, `LPT2`, `LPT3`, `LPT4`, `LPT5`, `LPT6`, `LPT7`, `LPT8`, `LPT9`

The user can select any name for *action-definition-file-name-after-conversion*, except that it cannot be the file name specified in the `-i` option. Furthermore, if a file that has the same name as the name of the file specified in the `-o` option, the `KAVB5504-E` message is displayed and the program terminates.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command checks the contents of the definition file to be converted by using regular expressions used by the specified logical host.

If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Notes

- If you use the `-i` or `-o` option to specify the automated action definition used in JP1/IM - Manager, do so after stopping JP1/IM - Manager.
- When a file is converted to the format of version 11-50 or later, some items become undefined. If such an undefined item is present, the `KAVB5505-W` message is displayed. Follow the directions in the message to correct the action definition file, and then use the `jcamakea` command to check that the definition file has been corrected successfully.

Return values

`0`	Normal termination
`1`	Abnormal termination
`2`	Termination with warning

Example

The following is an example of converting an action definition file that was created in the format of version 8 or earlier to the format of version 11-50 or later:

```
jcadefconv  -i actdef.conf  -o actdef_new.conf
```

The example assumes the following contents for the action definition file created in the format of version 8 or earlier:

```
DESC_VERSION=2
:state_watch=true
#comment
+0 $0000000A /message/,/basic-event-information/,/detailed-event-information
/,/-------E/ ATTR1=/attribute-value-1/ : u=user-name e=environment-variable
-file-name d=execution-host-name dt=20 rt=30 action
```

When the `jcadefconv` command is executed, the file is converted as follows:

```
DESC_VERSION=4
cmn
  sta true
end-cmn
act action-1
  aid action-ID
  valid true
  prm 0
  cmt comment
  eid A
  cnd
    B.MESSAGE REGEX message
    B.BASIC REGEX basic-event-information
    B.DETAIL REGEX detailed-event-information
    E.SEVERITY IN Emergency
    E.ATTR1 REGEX attribute-value-1
  end-cnd

  usr user-name
  hst execution-host-name
  cmd action
  var environment-variable-file-name
  det 20
  ret 30
end-act
```

jcamakea

Function

This command checks the definitions of automated actions. If the definitions span multiple automated action definition files, the command merges the files into one file. When multiple automated action definition files are to be merged, the command uses the version of the action definition file and the automated action status monitoring parameter that apply to the first file that is loaded.

The checking and merging results are output to standard output. The command checks the output results and creates the automated action definition file.

If the command detects errors during checking, it outputs error messages to standard error.

An automated action definition parameter in a specified automated action definition file that exceeds the maximum size is not output to standard output. For details about the size of an automated action definition parameter, see *Automated action definition file (actdef.conf)* in *Chapter 2. Definition Files*.

If a file contains no definition parameters or contains only comments, an error results.

Format

```
jcamakea [-h logical-host-name]automated-action-definition-file-name-1 [...a
utomated-action-definition-file-name-100]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that contains the regular expressions to be used to check the contents of the definition files that are to be converted. The command checks the contents of the definition files to be converted using the regular expressions used by the specified logical host. The command also checks whether any automated action definition file exceeds the maximum file size according to the file size settings in the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

automated-action-definition-file-name-1 [...*automated-action-definition-file-name-100*]

Specifies the relative or absolute path names of the files containing automated action definitions. You can specify a maximum of 100 files. Separate multiple file names with the space character. If the path name of an automated action definition file contains a space, enclose the entire path name in double quotation marks (").

A file name can consist of a maximum of 255 bytes.

Return values

0	Normal termination
3	Invalid argument
7	Format error or no permission
152	System error (in UNIX)
153	Insufficient memory (in UNIX)
154	File open error (in UNIX)
156	Logical error (in UNIX)
255	File open error (in UNIX)
-1	File open error (in Windows)
-100	Logical error (in Windows)
-102	File input/output error (in Windows)
-103	Insufficient memory (in Windows)
-104	System error (in Windows)

When the command reads an action definition file in the format of version 08-50 or earlier, it sets one of the following return values:

0: Normal termination

Other than 0: Abnormal termination

If multiple errors occur, the return value is for the last error that occurred.

Example

Merge automated action definition files `/usr/console/action1` and `/usr/console/action2` to create the automated action definition file `/usr/console/actionx1`:

```
jcamakea /usr/console/action1 /usr/console/action2 > /usr/console/actionx1
```

jcashowa

Function

This command displays the results of executing automated actions stored in an action information file. Automated action execution results can be displayed for an event that was registered at a specified date and time, or for all events that were registered during a specified period of time, or for all actions.

Format

```
jcashowa [-d {[MM/dd/hh:mm][, [MM/dd/hh:mm]]}]
         [-h logical-host-name]
         [action-information-file-name]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-d {[`*MM*`/`*dd*`/`*hh*`:`*mm*`][, [`*MM*`/`*dd*`/`*hh*`:`*mm*`]]}`

Specifies the time that the events subject to the actions stored in the action information file were registered. Use a comma (`,`) to separate the beginning date and time from the ending date and time. The command displays information about the actions for events that were registered during the specified period of time. When this option is omitted, the command displays information about all the actions stored in the action information file.

About the date/time specification (*MM*`/`*dd*`/`*hh*`:`*mm*):

You can use the formats shown in the table below for the date/time specification. Use the format appropriate to your operation.

Table 1–4: Date/time specification formats

Date/time specification pattern	Description
MM/*dd*/*hh*:*mm*	Specify month in *MM*, date in *dd*, hour in *hh*, and minute in *mm*.
MM/*dd*/*hh*	Specify month in *MM*, date in *dd*, and hour in *hh*. For the omitted *mm*, the command assumes `00`.
MM/*dd*	Specify month in *MM* and date in *dd*. For the omitted *hh* and *mm*, the command assumes `00` for both.
dd	Specify date in *dd*.

Date/time specification pattern	Description
	For the omitted *MM*, the command assumes the month the `jcashowa` command was executed. For *hh* and *mm*, the command assumes `00` for both.
dd/*hh*:*mm*	Specify date in *dd*, hour in *hh*, and minute in *mm*. For the omitted *MM*, the command assumes the month the `jcashowa` command was executed.
hh:*mm*	Specify hour in *hh* and minute in *mm*. For the omitted *MM*, the command assumes the month the `jcashowa` command was executed. For *dd*, the command assumes the date the `jcashowa` command was executed.

About the date/time range specification (`[`*MM*`/`*dd*`/`*hh*`:`*mm*`][, [`*MM*`/`*dd*`/`*hh*`:`*mm*`]]`*):*

You can use the formats shown in the table below for the date/time range specification. Use the format appropriate to your operation.

Table 1–5: Date/time range specification formats

Range specification pattern	Description
`-d` *datetime*	By specifying *datetime*, you can display the result of an action that was executed for an event registered at a specific date and time. For example, to display the result of an action that was executed for an event registered at 22:`00` on October 24, specify as follows: `jcashowa -d 10/24/22:00`
`-d` *datetime*`,`*datetime*	By specifying *datetime*`,`*datetime*, you can display the results of all actions that were executed for the events registered during a specified period (range) of time. For example, to display the results of the actions that were executed for all events registered from 22:00 on October 24 through 10:00 on November 24, specify as follows: `jcashowa -d 10/24/22:00,11/24/10:00`
`-d` *datetime*`,`	By specifying *datetime*`,`, you can display the results of all actions that were executed for the events registered on and subsequent to the specified date and time. For example, to display the results of the actions that were executed for the events registered at 22:00 on October 24 and thereafter, specify as follows: `jcashowa -d 10/24/22:00,`
`-d ,`*datetime*	By specifying `,`*datetime*, you can display the results of all actions that were executed for the events registered at and before the specified date and time. For example, to display the results of the actions that were executed for the events registered up to (and including) 10:00 on November 24, specify as follows: `jcashowa -d ,11/24/10:00`

About the default year:

If the specified beginning month value is greater than the value for the month during which the `jcashowa` command is executed, the command assumes the specified date and time belong to the previous year and treats the specification as being from the beginning date and time in the previous year to the ending date and time in the current year.

- When the specified beginning month value is greater than the value for the month during which the `jcashowa` command is executed:

  12 (December) ≥ value specified as the beginning month > value for the month during which the `jcashowa` command is executed

  The command assumes that the year for the specified beginning date and time is the year preceding the year during which the `jcashowa` command is executed.

- When the specified beginning month value is less than the value for the month during which the `jcashowa` command is executed:

Value for the month during which the `jcashowa` command is executed ≥ value specified as the beginning month ≥ 01 (January)

The command assumes that the year for the specified beginning date and time is the same as the year during which the `jcashowa` command is executed.

Example 1 (if the `jcashowa` command is executed on 2003/10/31):

```
# jcashowa -d 11/01/0:00,10/01/23:59
```

The command assumes the specified time range is from 2002/11/01 0:00 to 2003/10/01 23:59 and performs processing normally.

Example 2 (if the `jcashowa` command is executed on 2003/11/01):

```
# jcashowa -d 11/01/0:00,10/01/23:59
```

The command assumes the specified time range is from 2003/11/01 0:00 to 2003/10/01 23:59 and displays the message `KAVB4009-W` because the specified date and time are not in chronological order.

The specification of the `-d` option determines the chronicity of the specified dates/times. If the specified beginning and ending dates/times are not in chronological order, an error results.

About the seconds specification

For the seconds specification, 00 is assumed as the beginning time and 59 is assumed as the ending time.

Example 1 (if the `jcashowa` command is executed as follows):

```
# jcashowa -d 10/24/22:00
```

The results of actions executed from October 24, 22:00:00 to October 24, 22:00:59 are displayed.

Example 2 (if the `jcashowa` command is executed as follows):

```
# jcashowa -d 10/24/22:00,11/24/10:00
```

The results of actions executed from October 24, 22:00:00 to November 24, 10:00:59 are displayed.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command displays action execution results for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

action-information-file-name

Specifies the full path of the file to be used for the action information file.

If you specify an action information file at the physical host, do not specify the `-h` option or the `JP1_HOSTNAME` environment variable.

If you specify an action information file at the logical host, specify the logical host name in the `-h` option or the `JP1_HOSTNAME` environment variable.

The action information file name can consists of a maximum of 255 bytes.

The specified action information file will be used to store information about the executed actions.

This option must be the final option specified in the command. It must be specified after you have specified all other options that need to be specified.

Return values

0	Normal termination
3	Argument error
6	System error
7	No permission to execute the command (Windows)

Output format

When you execute the `jcashowa` command, automated action information is output in the following format:

`Event information`[#1] *event-IDΔserial-numberΔregistered-timeΔevent-arrival-time*

`Action information`[#2] *action-serial-numberΔaction-typeΔstatusΔdelay-statusΔPIDΔexecution-host-name*

`Action information` *action-inserted-timeΔaction-starting-timeΔaction-ending-timeΔreturn-code*

`Command` *command*

`Message` *message*

#1

If an AND condition is specified in the automated action settings, the command outputs only information about the last event received among all the events set in the execution condition.

#2

If no delay monitoring setting is specified for the action or the action is not delayed, the command outputs the following information:

`Action information` *action-serial-numberΔaction-typeΔstatusΔPIDΔexecution-host-name*

The following table lists and described each item that is output.

Table 1–6: Automated action information output items

Item	Description
event-ID	Event ID, in the format *basic-code*:*extended-code*.
serial-number	Serial number of the event.
registered-time	Event registration time, in the format *month*/*date* *hour*:*minute*:*second*.
event-arrival-time	Event arrival time, in the format *month*/*date* *hour*:*minute*:*second*.
action-serial-number	Action serial number of the action that is to be executed.
action-type	One of the following action types: • `Command` (command)
status	One of the following character strings indicating the action's execution status: • `running` (running) • `ended` (terminated) • `none` (none) • `fail` (not executable; error occurred before the execution request was passed to JP1/Base) • `error` (execution failed; error occurred within JP1/Base command control) • `unknown` (status unknown; command's execution result could not be determined) • `wait` (waiting for termination of the preceding command) • `send` (command is being transmitted) • `queue` (waiting for command execution in JP1/Base) • `cancel` (canceled) • `kill` (forced termination) • `deterrent` (suppressed) If the action is canceled from JP1/IM - View or by the `jcacancel` command, the cancellation status is displayed following the applicable status shown above. The action cancellation statuses are as follows:

Item	Description
	• `canceling` (being canceled). Example: `queue (canceling)` • `miss` (cancellation failed). Example: `ended (miss)` If the command is re-executed during a restart of the Automatic Action Service or the action is output to the action re-execution file, `-R` is appended to the above status (example: `ended-R`). If the action is re-executed from JP1/IM - View, `-RU` is appended to the above status (example: `ended-RU`). If a suppressed action is re-executed from JP1/IM - View, `-RUD` is appended to the above status (example: `ended-RUD`). If a suppressed action is re-executed from JP1/IM - View and then re-executed again or output to the action re-execution file because the Automatic Action Service was restarted (including node switching) during the re-execution, `-RD` is appended to the status (example: `ended-RD`). If a suppressed action's status is `fail` (not executable), `-D` is appended to `fail` (example: `fail-D`).
delay-status	Action's delay status. If the action is delayed, `delay` is displayed. If the action is not delayed, nothing is displayed.
PID	Process ID of the execution action. When action information is entered into the action re-execution file because of node switching, `OUTPUT` is displayed.
execution-host-name	Name of the host that executed the action.
action-inserted-time	Insertion time of the action to be executed, in the format *month*/*date* *hour*:*minute*:*second*. If the action has not been inserted, `**/** **:**:**` is displayed.
action-starting-time	Action start time, in the format *month*/*date* *hour*:*minute*:*second*. If the action has not started, `**/** **:**:**` is displayed.
action-ending-time	Action end time, in the format *month*/*date* *hour*:*minute*:*second*. If the action has not ended, `**/** **:**:**` is displayed.
return-code	Return code from the executed action. If the action has not ended, `***` is displayed.
command	Command executed as the action.
message	Message displayed by the command.

Example output

Example 1:

The command terminated abnormally and a message has been output:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 23000 Command ended 27934 raysol
Action information: 12/03 12:09:15 12/03 12:09:16
                    12/03 12:09:17 1
Command:            /usr/local/action
Message:            abc was not found.
```

Example 2:

Execution of the command is underway and no message has been output:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
```

```
Action information: 23000 Command running 27934 raysol
Action information: 12/03 12:09:15 12/03 12:09:16
                    **/** **:**:** ***
Command:           /usr/local/executing
```

Example 3:

The command status is `running`, the cancellation status is `canceling`, and no message has been output:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 10 Command running(canceling) 15236 raysol
Action information: 12/03 12:09:15 12/03 12:09:16
                    **/** **:**:** ***
Command:           /usr/local/action
```

Example 4:

There are results for multiple actions:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 380 Command ended 233 raysol
Action information: 12/03 12:09:13 12/03 12:09:14
                    12/03 12:09:14 20
Command:            /usr/local/action
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 381 Command ended 279 raysol
Action information: 12/05 10:39:20 12/05 10:39:21
                    12/05 10:39:23 128
Command:            /usr/local/action2
Message:            No permission
Execute as a superuser
Processing is canceled
```

Example 5:

There are multiple actions for a single event because a parameter group was specified:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 987 Command running 2904 raysol
Action information: 12/05 10:39:20 12/05 10:39:21
                    12/03 12:09:13 0
Command:            /usr/local/first
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 988 Command ended 2906 raysol
Action information: 12/05 10:39:20 12/05 10:39:21
                    12/06 21:02:54 0
Command:            /usr/local/second
```

Example 6:

Action information was entered in the action re-execution file due to node switching:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 45687 Command ended-R OUTPUT
Action information: **/** **:**:** *** **/** **:**:** ***
                    /****:**:** ***
```

Example 7:

The action being executed is delayed:

```
Event information:  00002000:00000000 20 12/03 12:03:26
                    12/03 12:03:26
Action information: 987 Command running delay 2904 raysol
Action information: 12/05 10:39:20 12/05 10:39:21
                    **/** **:**:** ***
Command:            /usr/local/executing
```

jcastatus

Function

Using standard output, this command displays the status (stopped, running, standby) of the automated action function that is running, and the contents of the automated action definition file that is loaded by the active automated action function.

Note that you can execute multiple instances of this command concurrently.

Format

```
jcastatus [-h logical-host-name]
          [-d]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command displays the status of the automated action function (Event Base Service) that corresponds to the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-d` (at Event Base Service)

Specifies that the contents of the automated action definition file that is loaded by the automated action function is displayed to standard output. The command displays the information in the same format as in the automated action definition file.

Even when all automated action definitions are disabled, the contents of the automated action definition file that is loaded by the active automated action function are displayed to standard output.

Return values

`0`	Normal termination
`4`	No response from the automated action function (Event Base Service)
`5`	Command cannot display the contents of the automated action definition file because the automated action function (Event Base Service) is stopped or on standby
`6`	System error (at the command)

`152`	System error (at Event Base Service) (in UNIX)
`154`	Input/output error (in UNIX)
`243`	A specified argument value was invalid (in UNIX)
`-13`	A specified argument value was invalid (in Windows)
`-102`	Input/output error (in Windows)
`-104`	System error (at Event Base Service) (in Windows)

Output format

When you execute the `jcastatus` command, the status of the automated action function is output in the following format:

```
Status : status
```

The following table describes the character strings that can be displayed as *status*.

Table 1–7: Statuses of the automated action function

Character string displayed in status	Status	Description
`STOP`	Stopped	The automated action function (Event Base Service) is stopped.
`RUNNING`	Running	The automated action function (Event Base Service) is running and available for use.
`STANDBY`	Standby	The Event Base Service is running, but the automated action function is in the standby mode. In this status, events are still received, but no action is taken on the received events. If the status changes from standby to running, action is not taken on the events that were received while in the standby mode.

Example output

The automated action function is in the standby mode:

```
Status : STANDBY
```

jcfaleltdef (Windows only)

Function

Defines the profile of a remote monitoring event log trap on the specified monitored host. The definition is overwritten whether the profile on the specified monitored host is running or has stopped.

To perform a batch reload, use the `jcfaleltdef` command to overwrite multiple running remote monitoring event log traps, and then use the `jcfaleltreload` command to batch-reload the profiles.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running.
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.

Format

```
jcfaleltdef -f remote-monitoring-event-log-trap-action-definition-file-name
            -o monitored-host-name
            [-filter filter]
            [-h logical-host-name]
```

Execution permission

Administrator permissions

Storage directory

Manager-path`\bin\imcf\`

Arguments

`-f` *remote-monitoring-event-log-trap-action-definition-file-name*

Specifies the name of an action definition file.

Specify the action definition file name as the full path or a relative path from the current directory with a maximum of 256 bytes. When specifying a relative path, do so in such a way that the full-path name with the directory name will not be more than 256 bytes.

The action definition file can be placed in any directory, and any file name can be specified.

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring event log trap whose profile you want to define. Note that the OS on the monitored host must be Windows.

`-filter` *filter*

Specifies the log type to filter on when the system has been set up to collect only event logs from a remotely monitored host.

When this option is specified, only event logs that match the specified log type are transferred to the manager. Specify this option to control the amount of log file data that is transferred from a remotely monitored host to the manager.

Use a character string in the following table to specify the log type. Note that the character strings are not case sensitive.

Specifiable log type	Log type of event logs to be filtered
Error	Error, Critical
Warning	Warning
Information	Information, Verbose
Audit_success	Security Audit Success
Audit_failure	Security Audit Failure

To specify multiple log types, use a comma (`,`) as a separator. Do not insert a space before or after the comma.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

Return values

`0`	Addition successful
`4`	Invalid argument
`6`	Unable to connect to the server
`7`	Invalid host information
`10`	Error in obtaining exclusive edit rights
`14`	Invalid DB
`17`	Invalid permission
`18`	Input/output error
`21`	Upper limit for number of concurrent executions reached
`255`	Internal error
Other value	Other error

Example 1

Add a profile on `host1`:

```
jcfaleltdef -f actionDefinition.conf -o host1
```

Example 2

Filter to obtain only the error, warning, and failed-audit event logs when a profile has been added on `host1`:

```
jcfaleltdef -f actionDefinition.conf -o host1 -filter Error,Warning,Audit_fa
ilure
```

jcfaleltreload (Windows only)

Function

Reloads remote monitoring event log traps. If trap processing is being performed when the command is executed, the traps are reloaded after the trap processing has finished. When a start option has been changed by using the `jcfaleltdef` command or the Display/Edit Profiles window, the change is not applied by the reload operation. Restart the system to apply the change.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running.
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- DCOM is set.
- A remote monitoring event log trap is running.

Format

```
jcfaleltreload {-o monitored-host-name | ALL}
               [-h logical-host-name]
```

Execution permission

Administrator permissions

Storage directory

Manager-path`\bin\imcf\`

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for the remote monitoring event log traps you want to reload. The OS on the monitored host must be Windows.

`ALL`

All remote monitoring event log traps are reloaded.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

Return values

0	Reloading successful
2	Partial or total failure
4	Invalid argument

6	Unable to connect to the server
7	Invalid host information
10	Error in obtaining exclusive edit rights
11	Invalid action definition file
12	Invalid authentication definition file
13	Communication error
14	Invalid DB
15	The specified remote monitoring event log trap has already stopped
17	Invalid permission
18	Input/output error
21	Upper limit for number of concurrent executions reached
255	Internal error
Other values	Other error

Example

Reload the remote monitoring event log trap on `host1`:

```
jcfaleltreload -o host1
```

jcfaleltstart (Windows only)

Function

Starts a remote monitoring event log trap.

Executing this command collects the event log files on the monitored host specified in the option, converts a line in a log file that satisfies the conditions specified in the action definition file of a remote monitoring event log trap to a JP1 event, and registers the event on an event server.

In order to specify the `-f` option, the action definition file of a remote monitoring event log trap must be created before the command is executed. Also, if the command is executed with the `-f` option specified and the profile has stopped, the existing action definition file of the remote monitoring event log trap is overwritten and the process for the trap profile is started. If the profile is running, the existing action definition file of the remote monitoring event log trap is overwritten and saved on the server, and an error message is displayed. At this point, the profile is running with the operation definition that existed before the action definition was overwritten.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- DCOM is set.

Format

```
jcfaleltstart
        -o monitored-host-name
        [-h logical-host-name]
        [-f remote-monitoring-event-log-trap-action-definition-file-name
        [-filter filter]]
```

Execution permission

Administrator permissions

Storage directory

Manager-path`\bin\imcf\`

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for the remote monitoring event log traps you want to start. The OS on the monitored host must be Windows.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

`-f` *remote-monitoring-event-log-trap-action-definition-file-name*

Specifies the name of an action definition file. If the `-f` option is specified, the existing action definition file of a remote monitoring event log trap is overwritten and started. If the `-f` option is not specified, the existing remote monitoring event log trap is started.

Specify the action definition file name as a full path or a relative path from the current directory with a maximum of 256 bytes. When specifying a relative path, do so in such a way that the full-path name with the directory name will be no more than 256 bytes.

The action definition file can be placed in any directory, and any file name can be specified.

`-filter` *filter*

Specifies a filter, when filters have already been set, according to log type to filter event logs acquired on a remotely monitored host. This option can be specified only when the `-f` option is specified.

When this option is specified, only event logs that match the specified log type are transferred to the manager. Specify this option to control the amount of log file data that is transferred from a remotely monitored host to the manager.

Use a character string in the following table to specify the log type. Note that the character strings are not case sensitive.

Specifiable log type	Log type of event logs to be filtered
Error	Error, Critical
Warning	Warning
Information	Information, Verbose
Audit_success	Security Audit Success
Audit_failure	Security Audit Failure

To specify multiple log types, use a colon (`,`) as a separator. Do not insert a space before or after the colon.

Return values

`0`	Trap started successfully
`4`	Invalid argument
`6`	Unable to connect to the server
`7`	Invalid host information
`8`	Already running
`9`	Profile threshold value exceeded
`10`	Error in obtaining exclusive edit rights
`11`	Invalid action definition file
`12`	Invalid authentication definition file
`13`	Communication error
`14`	Invalid DB
`17`	Invalid permission
`18`	Input/output error
`21`	Upper limit for number of concurrent executions reached
`255`	Internal error

Other values	Other error

Example 1

Start a remote monitoring event log trap on host1:

```
jcfaleltstart -o host1 -f actionDefinition.conf
```

Example 2

Filter to obtain only the error, warning, and failed-audit event logs when a remote monitoring event log trap on host1 is started:

```
jcfaleltstart -o host1 -f actionDefinition.conf -filter Error,Warning,Audit_
failure
```

jcfaleltstat (Windows only)

Function

Displays the operating status of a remote monitoring event log trap.

When this command is executed, the operating status of a remote monitoring event log trap that monitors the monitored host specified as the argument is returned.

If `ALL` is specified in the `-o` option and there is no host in the remote monitoring configuration, or if the OS is not Windows, a message indicating this status appears.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.

Format

```
jcfaleltstat {-o monitored-host-name | ALL}
             [-h logical-host-name]
```

Execution permission

Administrator permissions

Storage directory

Manager-path`\bin\imcf\`

Display format

When the `jcfaleltstat` command is executed, the output result is displayed in the format shown below.

`#`

In this example, the line number is added at the beginning of each line for descriptive purposes:

`1` *message-IDΔmessage*

`2` *message-IDΔmessage*

`3` *host-nameΔstatus*

`4` *host-nameΔstatus*

`5` *host-nameΔstatus*

`6` **:**

- Line 1
  A message indicating that command execution has started is displayed.

- Line 2
  A message indicating the following display scope is displayed:
  - All
  - Specified hosts
  - Specified event log traps on the specified host
- Lines 3 to 6
  The statuses related the event log traps on the remotely monitored hosts (Windows) for the specified scope are displayed. The following statuses are displayed:
  - `START`: The event log trap is running.
  - `STOP`: The event log trap has stopped.
  - `EDIT`: The action definition file for the event log trap is being edited, but the changes have not been applied.
  - `FAIL`: The event log trap status could not be obtained:
    - The host is invalid (host information was not collected, or collection failed))
    - An error occurred during WMI communication.
    - An authentication error occurred
    - An input/output error occurred.
    - An error occurred during an attempt to obtain exclusive rights.
    - An internal error occurred.

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring event log trap whose operating status you want to check. The OS on the monitored host must be Windows.

`ALL`

Checks the operating status of all remote monitoring event log traps.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

Return values

`0`	All remote monitoring event log traps are running
`1`	Some remote monitoring event log traps are running (when the `ALL` option is specified)
`2`	Partial or total failure
`4`	Invalid argument
`6`	Unable to connect to the server
`7`	Invalid host information
`14`	Invalid DB
`17`	Invalid permission
`18`	Input/output error

`19`	All remote monitoring event log traps have stopped.
`21`	Upper limit for number of concurrent executions reached
`255`	Internal error
Other values	Other error

Example

Display the operating status of a remote monitoring event log trap on `host1`:

```
jcfaleltstat -o host1
```

jcfaleltstop (Windows only)

Function

Stops remote monitoring event log traps.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- DCOM is set.
- A remote monitoring log file trap is running.

Format

```
jcfaleltstop {-o monitored-host-name | ALL}
             [-h logical-host-name]
```

Execution permission

Administrator permissions

Storage directory

Manager-path\bin\imcf\

Arguments

-o *monitored-host-name*

Specifies the name of the monitored host for the remote monitoring event log traps you want to stop. The OS on the monitored host must be Windows.

ALL

Stops all remote monitoring event log traps.

-h *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the JP1_HOSTNAME environment variable is set. If no logical host name is set for JP1_HOSTNAME, the physical host name is set.

Return values

0	Stopped successfully
2	Partial or total failure
4	Invalid argument
6	Unable to connect to the server
7	Invalid host information

10	Error in obtaining exclusive edit rights
12	Invalid authentication definition file
13	Communication error
14	Invalid DB
15	The specified remote monitoring event log trap has already stopped
17	Invalid permission
18	Input/output error
21	Upper limit for number of concurrent executions reached
255	Internal error
Other values	Other error

Example

Stop all remote monitoring event log traps:

```
jcfaleltstop ALL
```

jcfallogdef

Function

Adds or deletes the profile of a remote monitoring log file trap on the specified monitored host. Specifying the `-f` option adds the profile, and specifying the `-d` option deletes the profile.

If an added profile has the same monitoring name as an existing profile on the specified monitored host, the action definition file is overwritten whether the profile is running or has stopped.

This command can be executed only when the profile specified for deletion has stopped.

To perform a batch reload, use the `jcfallogdef` command to overwrite multiple running remote monitoring log file traps, and then use the `jcfallogreload` command to batch-reload the profiles.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.

Format

```
jcfallogdef
        -a monitoring-name
        -o monitored-host-name
        [-h logical-host-name]
        {-f remote-monitoring-log-file-trap-action-definition-file-name
            -c character-encoding
            [-filter filter]
            [-m maximum-length-of-data-treated-as-event (bytes)]
            [-p log-data-output-source-program-name]
            [-r]
            [-t file-monitoring-interval (seconds)]
            log-file-name1 [...log-file-name32] |
         -d}
        [-q]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-a` *monitoring-name*

Specifies the monitoring name used to identify a remote monitoring log file trap.

Specify a character string with a maximum of 30 bytes for the monitoring name. Alphanumeric characters, hyphens (`-`), and underlines can be used. The first character must be an alphanumeric character. The monitoring name is not case sensitive.

A paired monitoring name and monitored host must be unique, and cannot be the same as another pair specified by `jcfallogstart`. Note, however, that the same monitoring name as the one specified by `jevlogstart` of JP1/Base can be used.

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring log file trap to which you want to add or from which you want to delete a profile.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

`-f` *remote-monitoring-log-file-trap-action-definition-file-name*

Specifies the name of an action definition file.

Specify the action definition file name as a full path or a relative path from the current directory with a maximum of 256 bytes. When specifying a relative path, do so in such a way that the full-path name with the directory name will be no more than 256 bytes.

The action definition file can be placed in any directory, and any file name can be specified.

`-c` *character-encoding*

Specifies the character encoding of a log file. This option can be specified only when the `-f` option is specified.

You can specify the following character encodings.

Table 1–8: Character codes

OS	Japanese	English	Chinese
AIX	• SJIS When SJIS is specified, SJIS/Ja_JP is set. • SJIS/Ja_JP • SJIS/Ja_JP.IBM-932 • EUC When EUC is specified, EUC/ja_JP is set. • EUC/ja_JP • EUC/ja_JP.IBM-eucJP • UTF-8 When UTF-8 is specified, UTF-8/JA_JP is set. • UTF-8/JA_JP • UTF-8/JA_JP.UTF-8 • C	• C	• `GB18030` When `GB18030` is specified, `GB18030/Zh_CN.GB18030` is set. • `GB18030/Zh_CN.GB18030` • `GB18030/Zh_CN` • `UTF-8` When `UTF-8` is specified, `UTF-8/ZH_CN` is set. • `UTF-8/ZH_CN` • `UTF-8/ZH_CN.UTF-8` • `C`
HP-UX	• SJIS When SJIS is specified, SJIS/ja_JP.SJIS is set.	• C	• `GB18030` When `GB18030` is specified, `GB18030/zh_CN.gb18030` is set.

OS	Japanese	English	Chinese
	- SJIS/ja_JP.SJIS - SJIS/japanese - EUC When EUC is specified, EUC/ja_JP.eucJP is set. - EUC/ja_JP.eucJP - EUC/japanese.euc - UTF-8 When UTF-8 is specified, UTF-8/ja_JP.utf8 is set. - UTF-8/ja_JP.utf8 - C		- `GB18030/zh_CN.gb18030` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh_CN.utf8` is set. - `UTF-8/zh_CN.utf8` - `C`
Linux	- UTF-8 When UTF-8 is specified, UTF-8/ja_JP.UTF-8 is set. - UTF-8/ja_JP.UTF-8 - UTF-8/ja_JP.utf8 - SJIS#1 If SJIS is specified, SJIS/ja_JP.sjis is set. - SJIS/ja_JP.sjis#1 - SJIS/ja_JP.SJIS#1 - C	- UTF-8 When UTF-8 is specified, UTF-8/en_US.UTF-8 is set. - UTF-8/en_US.UTF-8 - UTF-8/en_US.utf8 - C	- `GB18030` When `GB18030` is specified, `GB18030/zh_CN.gb18030` is set. - `GB18030/zh_CN.gb18030` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh_CN.utf8` is set. - `UTF-8/zh_CN.utf8` - `C`
Solaris	- EUC When EUC is specified, EUC/ja is set. - EUC/ja - EUC/japanese - EUC/ja_JP.eucJP - SJIS When SJIS is specified, SJIS/ja_JP.PCK is set. - SJIS/ja_JP.PCK - UTF-8 When UTF-8 is specified, UTF-8/ja_JP.UTF-8 is set. - UTF-8/ja_JP.UTF-8 - C	- C	- `GB18030` When `GB18030` is specified, `GB18030/zh_CN.GB18030` is set. - `GB18030/zh_CN.GB18030` - `GB18030/zh_CN.GB18030@pinyin` - `GB18030/zh_CN.GB18030@radical` - `GB18030/zh_CN.GB18030@stroke` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh.UTF-8` is set. - `UTF-8/zh.UTF-8` - `UTF-8/zh_CN.UTF-8` - `UTF-8/zh_CN.UTF-8@pinyin` - `UTF-8/zh_CN.UTF-8@radical` - `UTF-8/zh_CN.UTF-8@stroke` - `C`
Windows	- SJIS	- SJIS#2 - C	- `GB18030`

#1

Valid only when the monitored OS is SUSE Linux.

#2

If the product runs on an English OS, the character encoding is `C` even if you specify `SJIS` for the character encoding.

`-filter` *filter*

Specifies a filter, when filters have already been set, that uses regular expressions to filter log files obtained on a remotely monitored host.

When this option is specified, only log data that matches the specified regular expressions is transferred to the manager. Specify this option to control the amount of log file data that is transferred from a remotely monitored host to the manager.

This option can be specified only when the `-f` option is specified.

This option is valid only when the OS on the remotely monitored host is UNIX. As a prerequisite condition, the `grep` command must be able to be executed over a SSH connection. When the OS on the remotely monitored host is Windows and this option is specified, it is ignored.

The regular expression formats that can be specified are the same as the formats of the extended regular expressions that can be specified in the `-E` option for the `grep` command on the remotely monitored host. No environment variables can be used.

Specify a character string with a maximum of 128 bytes for regular expressions. Characters that can be specified in the string are `'`, `"`, <, >, alphanumeric characters (excluding control characters), spaces, and symbols. If the character string contains a space, the entire string must be enclosed in double quotation marks (`"`).

Path examples for the `grep` command are given below. For details, see the documentation about the `grep` command in the applicable OS.

- For Linux: `/bin/grep`
- For Solaris: `/usr/xpg4/bin/grep`
- For an OS other than Linux and Solaris: `/usr/bin/grep`

`-m` *maximum-length-of-data-treated-as-event* (bytes)

Specifies the number of bytes to be read from the beginning of a line in a log file. From `1` to `1,024` bytes can be specified. If this option is omitted, `512` is set.

The last character in the line is converted to the `\0` symbol and indicates the end of the line. If a line in a log file exceeds the number of bytes specified for this option, the last byte is converted to `\0`.

The value specified for this option indicates the valid length of a line in the entered log file. Therefore, ensure that the regular expressions in the `MARKSTR` parameter in the action definition file of a remote monitoring log file trap and the regular expressions in the `ACTDEF` parameter are within the length specified here. In short, if there are any regular expressions corresponding to a column that exceed the valid length, they are not checked.

`-p` *log-data-output-source-program-name*

Specifies the name of the program to which log data is output. The specified name is displayed in the Event Console window of JP1/IM - View.

The following names are displayed.

In Windows:

`/HITACHI/JP1/NT_LOGTRAP/`*log-data-output-source-program-name*

In UNIX:

`/HITACHI/JP1/UX_LOGTRAP/`*log-data-output-source-program-name*

If this option is omitted, `/HITACHI/JP1/NT_LOGTRAP` is displayed for Windows and `/HITACHI/JP1/UX_LOGTRAP` is displayed for UNIX.

`-r`

If this option is omitted and any of the following cases apply, the system tries to collect data at the interval specified in the `-t` option until the log data can be collected.

- The remotely monitored host cannot be accessed when the remote monitoring log file trap starts.
- The remotely monitored host cannot be accessed while the remote monitoring log file trap is running
- The log file that is to be monitored cannot be accessed when the remote monitoring log file trap starts
- The log file that is to be monitored cannot be accessed while the remote monitoring log file trap is running

Specify the `-r` option for the following cases:

- The remotely monitored host can be accessed after the remote monitoring log file trap starts.
- The log file that is to be monitored is created after a remote monitoring log file trap starts.
- You want to continue monitoring the remotely monitored host even if it cannot be accessed.

If this option is omitted, one or the other of the following occurs:

- If the log file that is to be monitored cannot be obtained when the remote monitoring log file trap starts, the startup process stops and processing terminates.
- If the log file that is to be monitored cannot be collected while it is running, retry is attempted for the number of times specified in the action definition file for the log file trap at the interval specified in the file.

`-t` *file-monitoring-interval* (seconds)

Specifies the file monitoring interval. A value from `60` to `86,400` (seconds) can be specified. If this option is omitted, `300` is set.

When a log file in WRAP2 format is monitored

If wrap-around is performed frequently or a long monitoring interval is specified, the remote monitoring log file trap is overwritten before it reads data, causing some data to be lost. To prevent unread data, use the following formula for the monitoring interval:

log-file-size (bytes) × *number-of-log-files* > *output-size-per-second* (bytes) × *monitoring-interval* (seconds)

log-file-name`1 [...`*log-file-name*`32]`

Specifies the names of the log files to be monitored. Specify a character string with a maximum of 256 bytes for a log file name. If the monitored host OS is Windows, use the network path name without the host name for specification. If the OS is UNIX, use the full-path name. Note that wildcard characters cannot be specified for a log file to be monitored.

For a monitored host running UNIX, only log files with file paths consisting of alphanumeric characters, hyphens (`-`), underscores (`_`), periods (`.`), and slashes (`/`) can be monitored. File paths that include any other characters might not be monitored correctly.

A maximum of 32 files, and the following file formats, can be specified:

- Sequential file (SEQ)
- Sequential file (SEQ2)
- Wrap around file (WRAP2)

`-d`

Deletes the profile of a remote monitoring log file trap.

Because specifying this option deletes the remote monitoring log file trap from the profile tree, a message is displayed to confirm that there is no problem.

`-q`

If this option is specified, no confirmation message is displayed when the `-d` option is specified. If `-d` option is not specified, this option is ignored.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

- /*shared-directory-name*/jp1imm
- /*shared-directory-name*/jp1imm/log
- /*shared-directory-name*/jp1imm/log/imcf

Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

0	Addition or deletion successful
4	Invalid argument
6	Unable to connect to the server
7	Invalid host information
8	The specified monitoring name is already running (when the -d option is specified)
9	Profile threshold value exceeded
10	Error in obtaining exclusive edit rights
14	Invalid DB
17	Invalid permission
18	Input/output error
21	Upper limit for number of concurrent executions reached
255	Internal error
Other values	Other error

Example 1

Add a profile on host1:

```
jcfallogdef -a name1 -o host1 -f actionDefinition.conf -c SJIS -filter ".*-E
" /log/sample.log
```

Example 2

Delete a profile on host1:

```
jcfallogdef -a name1 -o host1 -d -q
```

jcfallogreload

Function

Reloads the action definition file of a remote monitoring log file trap.

The only definition information you can reload is that specified by the `MARKSTR` and `ACTDEF` parameter values of the action definition file. If a value other than the `MARKST` and `ACTDEF` parameter values is changed by using the `jcfallogdef` command or the Display/Edit Profiles window, the change is not applied by reloading the definition file. Restart the system to apply the change. Also, if the reload command is executed at the same time trap processing is executed, the information to be reloaded is applied to the trap processing.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- For SSH communication, SSH authentication can be performed by using the applicable remotely monitored host and public key encryption.
- For NetBIOS (NetBIOS over TCP/IP) communication, the log file to be monitored is shared.
- A remote monitoring log file trap is being started.

Format

```
jcfallogreload {-o monitored-host-name [-a monitoring-name] | ALL}
               [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:
Manager-path`\bin\imcf\`

In UNIX:
`/opt/jp1imm/bin/imcf/`

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring log file trap you want to reload.

`-a` *monitoring-name*

Specifies the monitoring name of a remote monitoring log file trap you want to reload.

Specify a character string with a maximum of 30 bytes for the monitoring name. Alphanumeric characters, hyphens (`-`), and underlines can be used. The first character must be an alphanumeric character. The monitoring name is not case sensitive.

`ALL`

Reloads the action definition file of each remote monitoring log file trap.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`
  - `/`*shared-directory-name*`/jp1imm/log`
  - `/`*shared-directory-name*`/jp1imm/log/imcf`

  Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	Reloading successful
`2`	Partial or total failure
`4`	Invalid argument
`6`	Unable to connect to the server
`7`	Invalid host information
`10`	Error in obtaining exclusive edit rights
`11`	Invalid action definition file
`12`	Invalid authentication definition file
`13`	Communication error
`14`	Invalid DB
`15`	The specified remote monitoring log file trap is already ended
`17`	Invalid permission
`18`	Input/output error
`21`	Upper limit for number of concurrent executions reached
`255`	Internal error

Other values	Other error

Example

Reload the remote monitoring log file trap `name1` on `host1`:

```
jcfallogreload -o host1 -a name1
```

jcfallogstart

Function

Starts a remote monitoring log file trap.

Executing this command collects log files on a monitored host, and sets a line in a log file that matches the conditions in the action definition file of the remote monitoring log file trap as a JP1 event. The event is then registered on an event server.

Specifying the `-f` option adds a new profile for a remote monitoring log file trap, and then starts a process. If a profile with the same monitoring name already exists on the specified monitored host when the profile has stopped, the trap's action definition file is overwritten, and a remote monitoring log file trap process is started. If the profile is running, the action definition file is overwritten and saved on the server, and an error message is displayed before the process stops. At this point, the profile is running with the operation definition that existed before the action definition was overwritten. If the `-f` option is not specified, the profile process for an existing remote monitoring log file trap is started.

Log files in different data formats cannot be processed together. For such cases, start a separate remote monitoring log file trap for each format.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- For SSH communication, SSH authentication can be performed by using the applicable remotely monitored host and public key encryption.
- For NetBIOS (NetBIOS over TCP/IP) communication, the log file to be monitored is shared.

Format

```
jcfallogstart
        -a monitoring-name
        -o monitored-host-name
        [-h logical-host-name]
        [-f remote-monitoring-log-file-trap-action-definition-file-name
          -c character-encoding
          [-filter filter]
          [-m maximum-length-of-data-treated-as-event (bytes)]
          [-p log-data-output-source-program-name]
          [-r]
          [-t file-monitoring-interval (seconds)]
          log-file-name1[ ...log-file-name32]]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-a` *monitoring-name*

Specifies the monitoring name used to identify the remote monitoring log file trap.

Specify a character string with a maximum of 30 bytes for the monitoring name. Alphanumeric characters, hyphens (`-`), and underlines can be used. The first character must be an alphanumeric character. The monitoring name is not case sensitive.

A paired monitoring name and a monitored host must be unique, and cannot be the same as another pair specified by `jcfallogstart`. Note, however, that the same monitoring name as the one specified by `jevlogstart` of JP1/Base can be used.

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring log file trap you want to start.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

`-f` *remote-monitoring-log-file-trap-action-definition-file-name*

Specifies the name of the action definition file as a full path or a relative path from the current directory with a maximum of 256 bytes. When specifying a relative path, do so in such a way that the full-path name with the directory name will be no more than 256 bytes.

The action definition file can be placed in any directory, and any file name can be specified.

Specifying this option creates a new remote monitoring log file trap and starts it. If this option is omitted, an existing remote monitoring log file trap is started.

`-c` *character-encoding*

Specifies the character encoding of a log file. This option can be specified only when the `-f` option is specified.

The following character encodings can be specified.

Table 1–9: Character codes

OS	Japanese	English	Chinese
AIX	• SJIS When SJIS is specified, SJIS/Ja_JP is set. • SJIS/Ja_JP • SJIS/Ja_JP.IBM-932 • EUC When EUC is specified, EUC/ja_JP is set. • EUC/ja_JP • EUC/ja_JP.IBM-eucJP • UTF-8	• C	• `GB18030` When `GB18030` is specified, `GB18030/Zh_CN.GB18030` is set. • `GB18030/Zh_CN.GB18030` • `GB18030/Zh_CN` • `UTF-8` When `UTF-8` is specified, `UTF-8/ZH_CN` is set. • `UTF-8/ZH_CN` • `UTF-8/ZH_CN.UTF-8` • `C`

OS	Japanese	English	Chinese
	When UTF-8 is specified, UTF-8/JA_JP is set. - UTF-8/JA_JP - UTF-8/JA_JP.UTF-8 - C		
HP-UX	- SJIS When SJIS is specified, SJIS/ja_JP.SJIS is set. - SJIS/ja_JP.SJIS - SJIS/japanese - EUC When EUC is specified, EUC/ja_JP.eucJP is set. - EUC/ja_JP.eucJP - EUC/japanese.euc - UTF-8 When UTF-8 is specified, UTF-8/ja_JP.utf8 is set. - UTF-8/ja_JP.utf8 - C	- C	- `GB18030` When `GB18030` is specified, `GB18030/zh_CN.gb18030` is set. - `GB18030/zh_CN.gb18030` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh_CN.utf8` is set. - `UTF-8/zh_CN.utf8` - `C`
Linux	- SJIS/ja_JP.sjis#1 - SJIS/ja_JP.SJIS#1 - UTF-8 When UTF-8 is specified, UTF-8/ja_JP.UTF-8 is set. - UTF-8/ja_JP.UTF-8 - UTF-8/ja_JP.utf8 - C	- UTF-8 When UTF-8 is specified, UTF-8/en_US.UTF-8 is set. - UTF-8/en_US.UTF-8 - UTF-8/en_US.utf8 - C	- `GB18030` When `GB18030` is specified, `GB18030/zh_CN.gb18030` is set. - `GB18030/zh_CN.gb18030` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh_CN.utf8` is set. - `UTF-8/zh_CN.utf8` - `C`
Solaris	- EUC When EUC is specified, EUC/ja is set. - EUC/ja - EUC/japanese - EUC/ja_JP.eucJP - SJIS When SJIS is specified, SJIS/ja_JP.PCK is set. - SJIS/ja_JP.PCK - UTF-8 When UTF-8 is specified, UTF-8/ja_JP.UTF-8 is set. - UTF-8/ja_JP.UTF-8 - C	- C	- `GB18030` When `GB18030` is specified, `GB18030/zh_CN.GB18030` is set. - `GB18030/zh_CN.GB18030` - `GB18030/zh_CN.GB18030@pinyin` - `GB18030/zh_CN.GB18030@radical` - `GB18030/zh_CN.GB18030@stroke` - `UTF-8` When `UTF-8` is specified, `UTF-8/zh.UTF-8` is set. - `UTF-8/zh.UTF-8` - `UTF-8/zh_CN.UTF-8` - `UTF-8/zh_CN.UTF-8@pinyin` - `UTF-8/zh_CN.UTF-8@radical` - `UTF-8/zh_CN.UTF-8@stroke` - `C`
Windows	- SJIS	- SJIS#2 - C	- `GB18030`

#1

Valid only when the monitored OS is SUSE Linux.

#2

If the product runs on an English OS, the character encoding is `C` even if you specify `SJIS` for the character encoding.

`-filter` *filter*

Specifies a filter, when filters have already been set, that uses regular expressions to filter log files obtained on a remotely monitored host.

When this option is specified, only log data that matches the specified regular expressions is transferred to the manager. Specify this option to control the amount of log file data that is transferred from a remotely monitored host to the manager.

This option can be specified only when the `-f` option is specified.

This option is valid only when the OS on the remotely monitored host is UNIX. As a prerequisite condition, the `grep` command must be able to be executed over an SSH connection. When the OS on the remotely monitored host is Windows and this option is specified, it is ignored.

The regular expression formats that can be specified are the same as the formats of the extended regular expressions that can be specified in the `-E` option for the `grep` command on the remotely monitored host. No environment variables can be used.

Specify a character string with a maximum of 128 bytes for regular expressions. Characters that can be specified in the string are `'`, `"`, <, >, alphanumeric characters (excluding control characters), spaces, and symbols. If the character string contains a space, the entire string must be enclosed in double-quotation marks (`"`).

Path examples for the `grep` command are given below. For details, see the documentation about the `grep` command in the applicable OS.

- For Linux: `/bin/grep`
- For Solaris: `/usr/xpg4/bin/grep`
- For an OS other than Linux and Solaris: `/usr/bin/grep`

`-m` *maximum-length-of-data-treated-as-event* (bytes)

Specifies the number of bytes to be read from the beginning of a line in a log file. From `1` to `1,024` bytes can be specified. If this option is omitted, `512` is set.

The last character in the line is converted to the `\0` symbol and indicates the end of the line. If a line in a log file exceeds the number of bytes specified for this option, the last byte is converted to `\0`.

The value specified for this option indicates the valid length of a line in the entered log file. Therefore, ensure that the regular expressions in the `MARKSTR` parameter in the action definition file of a remote monitoring log file trap and the regular expressions in the `ACTDEF` parameter are within the length specified here. In short, if there are any regular expressions corresponding to a column that exceed the valid length, they are not checked.

`-p` *log-data-output-source-program-name*

Specifies the name of the program to which log data is output. The specified name is displayed in the Event Console window of JP1/IM - View.

The following names are displayed.

In Windows:

`/HITACHI/JP1/NT_LOGTRAP/`*log-data-output-source-program-name*

In UNIX:

`/HITACHI/JP1/UX_LOGTRAP/`*log-data-output-source-program-name*

If this option is omitted, `/HITACHI/JP1/NT_LOGTRAP` is displayed for Windows and `/HITACHI/JP1/UX_LOGTRAP` is displayed for UNIX.

`-r`

If this option is omitted and any of the following cases apply, the system tries to collect data at the interval specified in the `-t` option until the log data can be collected.

- The remotely monitored host cannot be accessed when the remote monitoring log file trap is started
- The remotely monitored host cannot be accessed while the remote monitoring log file trap is running
- The log file that is to be monitored cannot be accessed when the remote monitoring log file trap is started
- The log file that is to be monitored cannot be accessed while the remote monitoring log file trap is running

Specify the `-r` option for the following cases:

- The remotely monitored host can be accessed after the remote monitoring log file trap starts.
- The log file that is to be monitored is created after a remote monitoring log file trap starts.
- You want to continue monitoring a remotely monitored host even if you cannot access it.

If this option is omitted, one or the other of the following occurs:

- If the log file that is to be monitored cannot be obtained when the remote monitoring log file trap starts, the startup process stops and processing terminates.
- If the log file that is to be monitored cannot be collected while it is running, retry is attempted for the number of times specified in the action definition file for the log file trap at the interval specified in the file.

`-t` *file-monitoring-interval* (seconds)

Specifies the file monitoring interval. A value from `60` to `86,400` (seconds) can be specified. If you omit this option, `300` is set.

When a log file in WRAP2 format is monitored

If wrap-around is performed frequently or a long monitoring interval is specified, the remote monitoring log file trap is overwritten before it reads data, causing some data to be lost. To prevent unread data, use the following formula for the monitoring interval:

log-file-size (bytes) × *number-of-log-files* > *output-size-per-second* (bytes) × *monitoring-interval* (seconds)

log-file-name`1 [...`*log-file-name*`32]`

Specifies the names of the log files to be monitored. Specify a character string with a maximum of 256 bytes for the log file name. If the monitored host OS is Windows, use the network path name without the host name for specification. If the OS is UNIX, use the full-path name. Note that wildcard characters cannot be specified for the log file to be monitored.

For a monitored host running UNIX, only log files with file paths consisting of alphanumeric characters, hyphens (`-`), underscores (`_`), periods (`.`), and slashes (`/`) can be monitored. File paths that include any other characters might not be monitored correctly.

A maximum of 32 files, and the following file formats, can be specified:

- Sequential file (SEQ)
- Sequential file (SEQ2)
- Wrap around file (WRAP2)

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`

- /*shared-directory-name*/jp1imm/log
- /*shared-directory-name*/jp1imm/log/imcf

Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

0	Trap started successfully
4	Invalid argument
6	Unable to connect to the server
7	Invalid host information
8	The specified monitoring name is already running
9	Profile threshold value exceeded
10	Error in obtaining exclusive edit rights
11	Invalid action definition file
12	Invalid authentication definition file
13	Communication error
14	Invalid DB
17	Invalid permissions
18	Input/output error
21	Upper limit for number of concurrent executions reached
255	Internal error
Other values	Other error

Example 1

Start the remote monitoring log file trap `monitoringName` on `host1`:

```
jcfallogstart -a monitoringName -o host1
```

Example 2

Create a new action definition file for a remote monitoring log file trap and start it:

```
jcfallogstart -a monitoringName -o host2 -f actionDefinition.conf -c SJIS -f
ilter ".*-E" /log/sample.log
```

jcfallogstat

Function

Displays the operating status of a remote monitoring log file trap.

Executing this command returns the operating status of a remote monitoring log file trap that has the monitoring name specified as the argument or that monitors the monitored host specified as the argument.

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.

Format

```
jcfallogstat {-o monitored-host-name [-a monitoring-name] | ALL}
             [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Display format

Executing the `jcfallogstat` command displays the output result in the format described below. Note that when `ALL` is specified and there are no hosts in the remote monitoring configuration, or when the specified host does not exist in the remote monitoring configuration, a message to that effect is displayed.

Note:

In this example, a line number is added at the beginning of each line for descriptive purposes:

1 *message-ID*Δ*message*

2 *message-ID*Δ*message*

3 [*host-name*]

4 *monitoring-name*Δ*status*

5 *monitoring-name*Δ*status*

```
6  monitoring-nameΔstatus

7  [host-name]

8  [host-name]

9  Δstatus

10 :
```

- Line 1
  A message indicating that command execution has started is displayed.
- Line 2
  A message indicating the following display scope is displayed:
  - All
  - Specified host
  - Specified log file traps on the specified host
- Lines 3 to 6
  The statuses of the log file traps on the remotely monitored host for the specified scope are displayed. The following statuses are displayed:
  - `START`: The log file trap is running.
  - `STOP`: The log file trap has stopped.
  - `EDIT`: The action definition file for the log file trap is being edited, but the changes have not been applied.
  - `FAIL`: The log file trap status could not be obtained for one of the following reasons:
    - The host is invalid (host information was not collected, or collection failed).
    - An error occurred in SSH or WMI/NetBIOS (NetBIOS over TCP/IP) communication.
    - An authentication error occurred.
    - An input/output error occurred.
    - An error occurred during an attempt to obtain exclusive rights.
    - An internal error occurred.
- Line 7
  If no log file traps are defined, only the host name is displayed.
- Lines 8 and 9
  If an error has occurred on a host but the status could not be obtained, only `FAIL` is displayed.
- Line 10
  The statuses of log file traps on all remotely monitored hosts for the specified scope are displayed.

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring log file trap whose operating status you want to check.

`-a` *monitoring-name*

Specifies the monitoring name of a remote monitoring log file trap whose operating status you want to check.

Specify a character string with a maximum of 30 bytes for the monitoring name. Alphanumeric characters, hyphens (`-`), and underlines can be used. The first character must be an alphanumeric character. The monitoring name is not case sensitive.

`ALL`

Specifies the monitoring names of all log file traps.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name is set. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`
  - `/`*shared-directory-name*`/jp1imm/log`
  - `/`*shared-directory-name*`/jp1imm/log/imcf`

  Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	All remote monitoring log file traps are running
`1`	Some remote monitoring log file traps are running (When the `ALL` option is specified, or only the `-o` option is specified)
`2`	Partial or total failure
`4`	Invalid argument
`6`	Unable to connect to the server
`7`	Invalid host information
`14`	Invalid DB
`17`	Invalid permission
`18`	Input/output error
`19`	All remote monitoring log file traps have stopped
`21`	Upper limit for number of concurrent executions reached
`255`	Internal error
Other values	Other error

Example

Display the operating status of the remote monitoring log file trap `name1` on `host1`:

```
jcfallogstat -o host1 -a name1
```

jcfallogstop

Function

Stops remote monitoring log file traps.

The following options are provided:

- Period of time that traps stop (individually or batched)
- Whether stopped remote monitoring log file traps should be deleted

Note that a maximum of five commands can be executed concurrently.

The following conditions must be satisfied to execute this command:

- The IM Configuration Management service is running
- There is a remotely monitored host in the remote monitoring configuration.
- A remotely monitored host has already collected host information.
- For SSH communication, SSH authentication can be performed by using the applicable remotely monitored host and public key encryption.
- For NetBIOS (NetBIOS over TCP/IP) communication, the log file to be monitored is shared.
- A remote monitoring log file trap is running.

Format

```
jcfallogstop {-o monitored-host-name [-a monitoring-name] | ALL}
             [-d]
             [-h logical-host-name]
             [-q]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:
Manager-path`\bin\imcf\`

In UNIX:
`/opt/jp1imm/bin/imcf/`

Arguments

`-o` *monitored-host-name*

Specifies the name of the monitored host for a remote monitoring log file trap you want to stop.

`-a` *monitoring-name*

Specifies the monitoring name of a remote monitoring log file trap you want to stop.

Specify a character string with a maximum of 30 bytes for the monitoring name. Alphanumeric characters, hyphens (-), and underlines can be used. The first character must be an alphanumeric character. The monitoring name is not case sensitive.

`ALL`

Stops all remote monitoring log file traps.

`-d`

Specifying this option deletes the entry for the remote monitoring log file trap you want to stop from the profile tree.

If this option is used together with the `-a`, `-o`, or `ALL` option, multiple remote monitoring log file traps are removed from the profile tree. In this case, a message is output to confirm that there is no problem. If this option is used together with any other option, it is ignored.

`-h` *logical-host-name*

Specifies the name of the logical host on which you want to execute the command. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is set. If no logical host name is set for `JP1_HOSTNAME`, the physical host name is set.

`-q`

If this option is specified, a confirmation message is not displayed when the `-d` option is specified. If `-d` option has not been specified, this option is ignored.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named /*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - /*shared-directory-name*/`jp1imm`
  - /*shared-directory-name*/`jp1imm/log`
  - /*shared-directory-name*/`jp1imm/log/imcf`

  Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

0	Stopping or deletion successful
2	Partial or total failure
4	Invalid argument
6	Unable to connect to the server
7	Invalid host information
10	Error in obtaining exclusive edit rights
12	Invalid authentication definition file
13	Communication error
14	Invalid DB

15	The specified remote monitoring log file trap has already stopped (when the -d option is not specified)
17	Invalid permission
18	Input/output error
21	Upper limit for number of concurrent executions reached
255	Internal error
Other values	Other error

Example 1

Stop the remote monitoring log file trap name1 on host1:

```
jcfallogstop -o host1 -a name1
```

Example 2

Stop and then delete all remote monitoring log file traps:

```
jcfallogstop ALL -d
```

jcfcolvmesx

Function

This command acquires virtualization configuration information from VMware ESX and outputs it to a virtualization configuration information file.

In order to collect the virtual host name of a guest OS from VMware ESX, VMware Tools must be running on the guest OS. The virtual host name cannot be collected if VMware Tools is not installed or if it is installed but not running.

The virtual host name also cannot be collected if the guest OS itself is not running.

This command uses the interface of VMware Infrastructure SDK for communication.

Format

```
jcfcolvmesx
          [-m communication-type]
          -u user-ID
          [-p password]
          -c host-name [host-name]
          -o output-file-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-m` *communication-type*

Specifies the method used to communicate with VMware ESX.

If `https` is specified, HTTPS is used for communication with VMware ESX. If `http` is specified, HTTP is used for communication with VMware ESX.

If this option is omitted, the command uses HTTPS for communication.

`-u` *user-ID*

Specifies the user ID associated with the connection-target VMware ESX account.

The user ID must be a maximum of 256 characters. Neither the space nor the tab character can be specified.

`-p` *password*

Specifies the password for the user ID that was specified in the `-u` option.

The password must be a maximum of 256 characters. Neither the space nor the tab character can be specified.

If this option is omitted, the command assumes that there is no password.

`-c` *host-name* `[`*host-name*`]`

Specifies the names of hosts where VMware ESX is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-o` *output-file-name*

Specifies the relative or absolute path name of the virtualization configuration information file that is to store the configuration information collected from VMware ESX. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

`0`	Normal termination#1
`1`	Argument error
`2`	Insufficient memory
`3`	JavaVM start error occurred
`4`	Execution permission error (Windows only)
`5`	Command was not executed from the administrator console (Windows only)
`6`	Output file already exists
`7`	Acquisition of virtualization configuration information failed#2
`8`	An input/output error occurred
`99`	Other error

#1

The command terminates normally even when some of the virtualization configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–10: Header information (line 1)

Item	Output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`090100`
Character encoding	UTF-8 fixed

Table 1–11: Output items (lines beginning with line 2)

Item	Output value
Host_name	`Host_name`
VMM_host_name	`VMM_host_name`
Virtual_manager_type	`Virtual_manager_type`
Manager_version	`Manager_version`
Virtual_host_manager	`Virtual_host_manager`

Table 1–12: Output items (From line 3)

Item	Description
Host name	Host name
VMM host name	Name of the host where virtualization environment software is run. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtual_manager_type	Type of product that manages the virtualization configuration: • For VMware ESX: `ESX`
Manager_version	Version of the product that manages a virtualization configuration
Virtual_host_manager	Name of the host that manages the VMM host For `jcfcolvmesx`: a space

Example output

```
#VM,090100,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
Vm1,ESX1,,,
Vm2,ESX1,,,
ESX1,,ESX,4.0,
```

jcfcolvmhcsm

Function

This command acquires virtualization configuration information from HCSM, and outputs it to a virtualization configuration information file.

For details about the prerequisite conditions for executing this command, see *3.3.1(1) Prerequisites for managing a virtualization configuration* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jcfcolvmhcsm
          -u user-ID
          -p password
          [-port port-number]
          -c host-name [host-name]
          -o output-file-name
```

Execution permission

In Windows: Administrators permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-u` *user-ID*

Specifies the user ID of a connection-destination HCSM account. Specify a character string with a maximum of 255 bytes, excluding control characters, for the user ID.

`-p` *password*

Specifies the password for the user ID that is specified in the `-u` option. Specify a character string with a maximum of 255 bytes, excluding control characters, for the password.

`-port` *port-number*

Specifies the port number for communicating with the connection destination HCSM. Specify a numeric value with one-byte characters from 1 to 65535. If you omit this option, `23015` is assumed.

`-c` *host-name* `[`*host-name*`]`

Specifies the names of hosts where HCSM is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-o` *output-file-name*

Specifies the relative or absolute path name of the virtualization configuration information file that is to store the configuration information acquired from HCSM. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

`0`	Normal termination[#1]
`1`	Argument error
`2`	Insufficient memory
`3`	JavaVM start error occurred
`4`	Execution permission error
`5`	Command was not executed from the administrator console
`6`	Output file already exists
`7`	Acquisition of virtualization configuration information failed[#2]
`8`	An input/output error occurred
`99`	Other error

#1

The command terminates normally even when some of the virtualization configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–13: Header information (line 1)

Item	Output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`101000`
Character encoding	UTF-8 fixed

Table 1–14: Header information (line 2)

Item	Output value
Host name	`Host_name`
VMM host name	`VMM_host_name`
Virtualization management type	`Virtual_manager_type`
Virtualization management product version	`Manager_version`
Virtualization configuration management host	`Virtual_host_manager`

Table 1–15: Output items (From line 3)

Item	Description
Host name	Host name

Item	Description
VMM host name	Name of the host where virtualization environment software is running. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtualization management type	Type of the product that manages the virtualization configuration: For HCSM: `HCSM` For Hitachi Compute Blade logical partitioning feature: `Virtage`
Virtualization management product version	Version of the product that manages a virtualization configuration. When the virtualization management type is HCSM, the version of the external connection interface for HCSM is set. Note that if virtualization configuration information is acquired from HCSM, no versions can be acquired on a host whose virtualization management type is Virtage.
Virtualization configuration management host	Name of the host that manages a VMM host

Example output

```
#VM,101000,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
WIN-T0NFDNMQ29E,,HCSM,7.2,
10.197.62.41,,Virtage,,WIN-T0NFDNMQ29E
bs20071-1,10.197.62.41,,,
WIN-77MGIUCU8P0,,,,WIN-T0NFDNMQ29E
guest01,,,,WIN-T0NFDNMQ29E
```

jcfcolvmkvm

Function

This command acquires virtualization configuration information from KVM, and outputs it to a virtualization configuration information file.

For details about the prerequisite conditions for executing this command, see *3.3.1(1) Prerequisites for managing a virtualization configuration* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jcfcolvmkvm
          -u user-ID
          -i private-key-file-path
          [-port port-number]
          -c host-name [host-name]
          -o output-file-name
```

Execution permission

In Windows: Administrators permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-u` *user-ID*

Specifies the user ID of the host where the connection destination KVM is running. Specify a character string with a maximum of 255 bytes, excluding control characters, for the user ID.

`-i` *private-key-file-path*

Specifies the name of the private key file that is used to communicate with the connection destination KVM in absolute path format. Specify a character string with a maximum of 256 bytes, excluding control characters, for the private key file. The private key file path is case sensitive. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-port` *port-number*

Specifies the port number for an SSH connection with the connection destination KVM. Specify a numeric value with one-byte characters from 1 to 65535. If you omit this option, `22` is assumed.

`-c` *host-name* `[`*host-name*`]`

Specifies the names of hosts where KVM is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-o` *output-file-name*

Specifies the relative or absolute path name of the virtualization configuration information file that is to store the configuration information acquired from KVM. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

`0`	Normal termination[#1]
`1`	Argument error
`2`	Insufficient memory
`3`	JavaVM start error occurred
`4`	Execution permission error
`5`	Command was not executed from the administrator console
`6`	Output file already exists
`7`	Acquisition of virtualization configuration information failed[#2]
`8`	An input/output error occurred
`99`	Other error

#1

The command terminates normally even when some of the virtualization configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–16: Header information (line 1)

Item	Output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`101000`
Character encoding	UTF-8 fixed

Table 1–17: Header information (line 2)

Item	Output value
Host name	`Host_name`
VMM host name	`VMM_host_name`
Virtualization management type	`Virtual_manager_type`
Virtualization management product version	`Manager_version`
Virtualization configuration management host	`Virtual_host_manager`

Table 1–18: Output items (From line 3)

Item	Description
Host name	Host name

Item	Description
VMM host name	Name of the host where virtualization environment software is running. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtualization management type	Type of the product that manages the virtualization configuration: For KVM, `KVM` is output.
Virtualization management product version	Version of the product that manages a virtualization configuration.
Virtualization configuration management host	Name of the host that manages a VMM host. For the `jcfcolvmkvm` command, this field is always blank.

Example output

```
#VM,101000,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
jp1-sf7800b,,KVM,0.12.1,
kv7801,jp1-sf7800b,,,
kv7802,jp1-sf7800b,,,
kv7803,jp1-sf7800b,,,
kv7804,jp1-sf7800b,,,
```

jcfcolvmscvmm (Windows only)

Function

This command acquires virtualization configuration information from SCVMM and outputs it to a virtualization configuration information file.

For details about the prerequisite conditions for executing this command, see *3.3.1(1) Prerequisites for managing a virtualization configuration* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jcfcolvmscvmm
          -c host-name [host-name]
                   [-d domain name -u user-ID[-p password]]
          -o output-file-name
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Manager-path`\bin\imcf\`

Arguments

`-c` *host-name* `[`*host-name*`]`

Specifies the names of hosts where SCVMM is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-d` *domain name*

Specifies the name of the domain to which the connection-target SCVMM host belongs. This option can be omitted if JP1/IM - Manager belongs to the same domain as that of the connection-target SCVMM host. For a domain name, specify a maximum of 255 characters.

`-u` *user-ID*

Specifies the user ID of the administrator permission account for the domain to which the connection-target SCVMM host belongs. This option is optional, but if you specify the `-d` option, you must also specify this option. Specify a character string with a maximum of 255 bytes, excluding control characters, for the user ID.

`-p` *password*

Specifies the password for the user ID that is specified in the `-u` option. If this option is omitted, the command assumes that there is no password. Specify a character string with a maximum of 255 bytes, excluding control characters, for the password.

`-o` *output-file-name*

Specifies the name of the virtualization configuration information file that stores the configuration information obtained from vCenter in relative path or absolute path format. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

0	Normal termination[#1]
1	Argument error
2	Insufficient memory
3	JavaVM start error occurred
4	Execution permission error
5	Command was not executed from the administrator console
6	Output file already exists
7	Acquisition of virtualization configuration information failed[#2]
8	An input/output error occurred
99	Other error

#1

The command terminates normally even when some of the virtual configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–19: Header information (line 1)

Item	Description of output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`090100`
Character encoding	UTF-8 fixed

Table 1–20: Header information (line 2)

Item	Description of output value
Host_name	`Host_name`
VMM_host_name	`VMM_host_name`
Virtual_manager_type	`Virtual_manager_type`
Manager_version	`Manager_version`
Virtual_host_manager	`Virtual_host_manager`

Table 1–21: Output items (lines beginning with line 3)

Item	Description
Host_name	Host name
VMM_host_name	Name of the host where virtualization environment software is run. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtual_manager_type	Type of product that manages the virtualization configuration:

Item	Description
	• For Hyper-V: `Hyper-V` • For SCVMM: `SCVMM` • For vCenter: `vCenter` • For VMware ESX: `ESX`
Manager_version	Version of the product that manages a virtualization configuration
Virtual_host_manager	Name of the host that manages a VMM host

Example output

```
#VM,090100,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
Vm1,ESX1,,,
Vm2,ESX1,,,
ESX1,,ESX,4.0,vCenter1
vCenter1,, vCenter,2.0,SCVMM1
SCVMM1,,SCVMM,2008,
```

jcfcolvmvc

Function

Obtains virtualization configuration information from vCenter, and outputs it to a virtualization configuration information file.

For details about the prerequisite conditions for executing this command, see *3.3.1(1) Prerequisites for managing a virtualization configuration* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jcfcolvmvc
          [-m communication-type]
          -u user-ID
          [-p password]
          -c host-name [host-name]
          -o output-file-name
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-m` *communication-type*

Specifies the method of communication with vCenter.

When `https` is specified, https communication is used for communication with vCenter. When `http` is specified, http communication is used for communication with vCenter.

If this option is omitted, https communication is used.

`-u` *user-ID*

Specifies the user ID of a connection-target vCenter account.

Specify a character string with a maximum of 255 bytes, excluding control characters, for the user ID.

`-p` *password*

Specifies the password for the user ID that is specified in the `-u` option.

Specify a character string with a maximum of 255 bytes, excluding control characters, for the password.

If this option is omitted, the command assumes that there is no password.

`-c` *host-name* `[`*host-name*`]`

Specifies the names of the hosts where vCenter is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-o` *output-file-name*

Specifies the name of the virtualization configuration information file that stores the configuration information obtained from vCenter in relative path or absolute path format. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

`0`	Normal termination#1
`1`	Argument error
`2`	Insufficient memory
`3`	JavaVM start error occurred
`4`	Execution permission error
`5`	The command was not executed from the administrator console
`6`	Output file already exists
`7`	Acquisition of virtualization configuration information failed#2
`8`	Input/output error
`99`	Other error

#1

The command terminates normally even when some of the virtual configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–22: Header information (line 1)

Item	Output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`090100`
Character encoding	UTF-8 fixed

Table 1–23: Header information (line 2)

Item	Output value
Host name	`Host_name`
VMM host name	`VMM_host_name`
Virtualization management type	`Virtual_manager_type`
Virtualization management product version	`Manager_version`
Virtualization configuration management host	`Virtual_host_manager`

Table 1–24: Output items (From line 3)

Item	Description
Host name	Host name
VMM host name	Name of the host where virtualization environment software runs. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtualization management type	Type of product that manages the virtualization configuration: • For vCenter: `vCenter` • For VMware ESX: `ESX`
Virtualization management product version	Version of the product that manages a virtualization configuration
Virtualization management former host name	Name of the host that manages a VMM host

Example output

```
#VM,090100,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
Vm1,ESX1,,,
Vm2,ESX1,,,
ESX1,,ESX,4.0,vCenter1
vCenter1,, vCenter,2.0,
```

jcfcolvmvirtage

Function

This command acquires virtualization configuration information from Hitachi Compute Blade logical partitioning feature and outputs it to a virtualization configuration information file.

For the prerequisite conditions for executing this command, see *3.3.1(1) Prerequisites for managing a virtualization configuration* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jcfcolvmvirtage
          -c host-name [host-name]
          -o output-file-name
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console.)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-c` *host-name* `[`*host-name*`]`

Specifies the name of the host where JP1/SC/CM that manages Hitachi Compute Blade logical partitioning feature is running. For a host name, specify a maximum of 255 characters. You can specify multiple host names by separating them with the space character or the tab delimiter.

`-o` *output-file-name*

Specifies the virtualization configuration information file that stores the configuration information obtained from JP1/SC that manages Hitachi Compute Blade logical partitioning feature in relative path or absolute path format. This option cannot be omitted. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

0	Normal termination[#1]
1	Argument error
2	Insufficient memory
3	JavaVM start error occurred
4	Execution permission error
5	The command was not executed from the administrator console

`6`	Output file already exists
`7`	Acquisition of virtualization configuration information failed#2
`8`	Input/output error
`99`	Other error

#1

The command terminates normally even when some of the virtual configuration information has not been acquired.

#2

The command outputs a return value if it is unable to acquire virtualization configuration information from any host.

Format of the virtualization configuration information file

Table 1–25: Header information (line 1)

Item	Output value
Identification character string for a virtualization configuration information file	`#VM`
File format version	`090100`
Character encoding	UTF-8 fixed

Table 1–26: Header information (line 2)

Item	Output value
Host name	`Host_name`
VMM host name	`VMM_host_name`
Virtualization management type	`Virtual_manager_type`
Virtualization management product version	`Manager_version`
Virtualization configuration management host	`Virtual_host_manager`

Table 1–27: Output items (From line 3)

Item	Description
Host name	Host name
VMM host name	Name of the host where virtualization environment software runs. In the case of a VMM host with no guest OS, the virtual host name field is blank and only the VMM host name is set.
Virtualization management type	Type of product that manages the virtualization configuration: • For JP1/SC/CM: `JP1/SC/CM` • For Hitachi Compute Blade logical partitioning feature: `Virtage`
Virtualization management product version	Version of the product that manages a virtualization configuration
Virtualization management former host name	Name of the host that manages a VMM host

Example output

```
#VM,090100,UTF-8
Host_name,VMM_host_name,Virtual_manager_type,Manager_version,Virtual_host_ma
nager
```

```
Vm1,VIRTAGE1,,,
Vm2, VIRTAGE1,,,
VIRTAGE1,,Virtage,
SCCM1,VIRTAGE1,JP1/SC/CM,,
```

jcfdbsetup

Function

This command sets up the IM Configuration Management database for storing configuration information. You must have already specified in advance in the setup information file the database's size, port number, and storage location.

In Windows, if this command is executed in an environment where the integrated monitoring database is not set up, the following services are registered in the OS:

- When setting up a physical host: JP1/IM3-Manager DB Server, JP1/IM3-Manager DB Cluster Service
- When setting up a cluster configuration: JP1/IM3-Manager DB Server_*logical-host-name*, JP1/IM3-Manager DB Cluster Service_*logical-host-name*

In UNIX, if this command is executed in an environment where the integrated monitoring database is not set up, an entry containing the path to the IM database is added to the `/etc/inittab` file. The entry is added to the respective physical and logical hosts on which the command was executed. Do not delete, edit, or comment out the entry in the `/etc/inittab` file that is added when this command is executed.

Format

```
jcfdbsetup {-f setup-information-file-name|-s}
           [-h logical-host-name -c {online|standby}]
           [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-f` *setup-information-file-name*

Specifies the setup information file that contains the requisite information, such as the installation folder and the size of the database area. If neither an IM Configuration Management database nor an integrated monitoring database has been set up, you must specify this option. If the integrated monitoring database has already been set up, specify in this option the setup information file that you specified when you set up the integrated monitoring database. Alternatively, if the integrated monitoring database has already been set up, you can specify the `-s` option instead. In such a case, the command uses the setup information that was specified when the integrated monitoring database was set up.

This option cannot be specified together with the `-s` option. Additionally, the `-f` and `-s` options cannot both be omitted.

If the path contains a space, enclose the entire path in double-quotation marks ("). If you configure a cluster environment, specify the cluster setup information file name.

`-s`

If the integrated monitoring database has already been set up, you can specify this option instead of the `-f` option. When this option is specified, the command sets up the IM Configuration Management database using the setup information that was specified when the integrated monitoring database was set up.

If the integrated monitoring database has not been set up but this option is specified, the command displays the `KNAN11193-E` message.

This option cannot be specified together with the `-f` option. Additionally, the `-s` and `-f` options cannot both be omitted.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. The command sets up the IM Configuration Management database for the specified logical host. If you do not use a cluster system, specification of this option is not needed. Note that this logical host name cannot be `JP1_DEFAULT`. In addition, the logical host name is case sensitive. For the logical host name, specify a logical host name set in JP1/Base in the correct form, especially case.

`-c {online|standby}`

Specifies the setup type in the cluster configuration (primary node or secondary node). If you have specified the `-h` option, you must specify this option. In addition, if the integrated monitoring database has already been set up on the same host, for the `-c` option, specify the same value that you used when you created the integrated monitoring database.

- `online`: Specifies that the primary node is to be set up.
- `standby`: Specifies that the secondary node is to be set up.

If you specify `online`, mount the shared disk and establish a connection to the logical host. If you are running a logical host in a non-cluster environment, specify `online` in the `-c` option.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

`0`	Normal termination
`1`	Abnormal termination

Notes

- The contents of the cluster setup information files must be identical between the primary and secondary nodes. When you set up the secondary node, copy the cluster setup information file used for the primary node and then use that file. If the contents of the files specified for the primary and secondary nodes are different, cancel the setup at the secondary node, copy the cluster setup information file from the primary node, and then re-execute the command.
- If you execute the command with the `-c` option specified, do not switch servers during execution. If you switch servers during execution, cancel the setup after the command has terminated, and then re-execute the command.
- If you have canceled the command's execution by pressing **Ctrl** + **C** or **Ctrl** + **Break**, make sure that the `pdistup`, `pdfmkfs`, `pddef`, and `pdload` processes are not executing, execute the `jcfdbunsetup` command, and then re-execute this command.
- If the integrated monitoring database has already been set up and the IM database is being used, JP1/IM - Manager Service must be stopped.

- If you are using the integrated monitoring database in Windows, the IM database (JP1/IM3-Manager DB Server) must be running and the cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) must be stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command, verify that the logical host name specified in the argument matches the JP1/Base logical host name, and that the logical host name can be resolved.
- If you cancel setup of the IM database by executing the `jcodbunsetup` or `jcfdbunsetup` command, you must restart the OS before re-executing the `jcfdbsetup` command.
- Before executing the command in Windows , in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jcfdbunsetup

Function

This command cancels setup of the IM Configuration Management database that stores configuration information.

Execute this command when you stop using the IM Configuration Management database, uninstall JP1/IM - Manager, re-create the IM Configuration Management database, or expand the database size.

In an environment in which an integrated monitoring database has been set up, the integrated monitoring database is still available even after execution of this command.

In Windows, if this command is executed in an environment where the integrated monitoring database is not set up, the following services are deleted:

- When removing setup of a physical host: JP1/IM-Manager DB Server, JP1/IM-Manager DB Cluster Service
- When removing setup of a cluster configuration: JP1/IM-Manager DB Server_*logical-host-name*, JP1/IM-Manager DB Cluster Service_*logical-host-name*

In UNIX, if this command is executed in an environment where the integrated monitoring database is not set up, entries in the `/etc/inittab` file registered by the `jcodbsetup` or `jcfdbsetup` command are deleted. The entries that are deleted are only those for processing related to the physical and logical hosts on which the command was executed.

Note that the following files must be deleted after the `jcfdbunsetup` command has been executed.

In Windows:

For a physical host:

Manager-path`\data\imcf\`*file-under-imconfig*

Manager-path`\data\imcf\`*file-and-folder-under-profiles*

For a logical host:

shared-folder`\data\imcf\`*file-under-imconfig*

shared-folder`\data\imcf\`*file-and-folder-under-profiles*

In UNIX:

For a physical host:

`/var/opt/jp1imm/data/imcf/`*file-under-imconfig*

`/var/opt/jp1imm/data/imcf/`*file-and-folder-under-profiles*

For a logical host:

shared-directory`/data/imcf/`*file-under-imconfig*

shared-directory`/data/imcf/`*file-and-directory-under-profiles*

Format

```
jcfdbunsetup [-h logical-host-name -c {online|standby}]
             [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. The command cancels setup of the IM Configuration Management database for the specified logical host. If you do not use a cluster system, specification of this option is not needed. Note that this logical host name cannot be `JP1_DEFAULT`. In addition, the logical host name is case sensitive. For the logical host name, specify a logical host name set in JP1/Base in the correct form, especially case.

`-c {online|standby}`

Specifies the type of setup being canceled in the cluster configuration (primary node or secondary node). If you have specified the `-h` option, you must specify this option.

- `online`: Specify this value if you specified `online` during setup of the IM Configuration Management database.
- `standby`: Specify this value if you specified `standby` during setup of the IM Configuration Management database.

If you specify online, mount the shared disk and establish a connection to the logical host. If you cancel setup of the IM Configuration Management database on a logical host that was running in a non-cluster environment, specify `online` in the `-c` option.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

`0`	Normal termination
`1`	Abnormal termination

Notes

- If you want to expand the database size in an environment where the integrated monitoring database has been created, you must execute the command for performing unsetup of the integrated monitoring database after executing the `jcfdbunsetup` command.
- If you execute this command with the `-c` option specified, do not switch servers during execution. If you switch servers during execution, re-execute the command after it has terminated.
- If you have canceled the command's execution by pressing **Ctrl** + **C** or **Ctrl** + **Break**, make sure that the `pdirst` process is not executing, and then re-execute this command.
- In Windows, services must be in the following status:

For the physical host:

The cluster service for the IM database (JP1/IM3-Manager DB Cluster Service) must have stopped, and the IM database service (JP1/IM3-Manager DB Server) must have started. In addition, when the integrated monitoring database has been set up and the IM database is being used, the JP1/IM - Manager service (JP1/IM3-Manager) must have stopped.

For the logical host:

The cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) on the logical host must be stopped, and the IM database service (JP1/IM3-Manager DB Server_*logical-host-name*) on the logical host must be started. In addition, if the integrated monitoring database has been set up and the IM database is being used, the JP1/IM - Manager service (JP1/IM3-Manager_*logical-host-name*) must be stopped.

- In UNIX, when the IM Configuration Management database has been set up and the IM database is being used, the JP1/IM-Manager service must have stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jcfexport

Function

This command outputs the hierarchy configuration (IM configuration) of the system managed by IM Configuration Management, host information, and definition information.

When you execute this command, the three types of information (host, system hierarchy, and profiles) that have been managed by IM Configuration Management before import processing are all deleted and then the specified information is imported.

To use this command, IM Configuration Management Service must be running. This command cannot be executed while the `jcfimport` command is executing. A maximum of five commands can be executed concurrently.

Format

```
jcfexport         [-h logical-host-name]
                  [-f]
                  -o directory-name
                  [-m | -r | -c | -g | -a]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-f`

Specifies that the file is to be overwritten if the specified directory already contains a file with the same name as the export file. If this option is omitted and the export target already contains a file with the same name, the information is not exported.

`-o` *directory-name*

Specifies the name of the directory to which the export data is to be output, expressed as an absolute path or a path relative to the location where the command is executed. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-m`

Specifies that only the host information is to be exported. The exported information is output to the host input information file (`host_input_data.csv`).

This option cannot be specified together with the `-r`, `-c`, `-g`, or `-a` option. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-r`

Only host information and remote authentication information are exported.

This option cannot be specified together with the `-m`, `-c`, `-g`, or `-a` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-c`

Specifies that only the host information and the system hierarchy information is to be exported. The host information is output to the host input information file (`host_input_data.csv`), and the system hierarchy is output to `system_tree_information.txt`.

This option cannot be specified together with the `-m`, `-r`, `-g`, or `-a` option. If specified in such a case, an invalid argument error results. If you omit all of the `-m`, `-c`, and `-a` options, the `-a` option is assumed. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-g`

Only host information, business group information, and monitoring group information are exported.

This option cannot be specified together with the `-m`, `-r`, `-c`, or `-a` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-a`

Specifies that all three types of information are to be exported. The exported information is output to `data_information.txt`. The host information is output to the host input information file (`host_input_data.csv`), the system hierarchy is output to `system_tree_information.txt`, and the definition information is output to the following files directly under *directory-specified-in--o-option*`\definition_files\`*host-name*`\`*product-name*:

- Forwarding settings file (`forward`)
- The action definition file of a log file trap (an arbitrary file)
- Log file trap startup definition file (`jevlog_start.conf`)
- Event log trapping function operation definition file (`ntevent.conf`)
- Location action definition file (`jbslcact.conf`)

This option cannot be specified together with the `-m`, `-r`, `-c`, or `-g` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

Notes

- For hosts where no profile configuration file is collected, there is no data to be exported (and no directory is created).
- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`

- /*shared-directory-name*/jp1imm/log
- /*shared-directory-name*/jp1imm/log/imcf

Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	Normal termination
`4`	Invalid option
`8`	Server cannot be connected
`12`	Memory shortage occurred
`16`	Invalid permission
`20`	Error, such as a file error, invalid path, or file already exists
`21`	Upper limit for number of concurrent executions reached
`24`	An input/output error occurred
`120`	System error occurred
`124`	Terminated due to other error
`201` or greater	JavaVM start error occurred

Example

Export all IM Configuration Management information to the directory under `c:\temp`:

```
jcfexport -o c:\temp
```

jcfimport

Function

This command imports IM Configuration Management information.

You cannot use this command unless IM Configuration Management Service is running. Note that this command cannot be executed during remote monitoring. In addition, a maximum of five commands can be executed concurrently.

Executing this command deletes three types of information (host, system hierarchy (IM configuration), and profile) that have been managed by IM Configuration Management before import processing. Thereafter, the information specified by options is imported.

To perform remote monitoring after the import, open the System Common Settings window from the IM Configuration Management - View, review the settings, and then click the **OK** button.

Format

```
jcfimport  [-h logical-host-name]
            -i directory-name
           [-m | -r | -c | -g | -a]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name. If you do not use a cluster system, there is no need to specify this option.

`-i` *directory-name*

Specifies the name of the directory to which files were exported by the `jcfexport` command, expressed as an absolute path or a path relative to the location where the `jcfimport` command is executed. This option is mandatory.

`-m`

Specifies that only the host information is to be imported. This option cannot be specified together with the `-c`, `-r`, `-g`, or `-a` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-r`

Imports only host information and remote authentication information.

This option cannot be specified together with the `-m`, `-c`, `-g`, or `-a` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-c`

Specifies that the system hierarchy and host information are to be imported. This option cannot be specified together with the `-m` or `-a` option. If specified in such a case, an invalid argument error results. If you omit all of the `-m`, `-c`, and `-a` options, the `-a` option is assumed.

`-g`

Imports host information, business group information, and monitoring group information only.

This option cannot be specified together with the `-m`, `-r`, `-c`, or `-a` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

`-a`

Specifies that all information is to be imported. This option cannot be specified together with the `-m`, `-r` `-c`, or `-g` option. If specified in such a case, an invalid argument error results. If all of the `-m`, `-r`, `-c`, `-g`, and `-a` options are omitted, the `-a` option is assumed.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`
  - `/`*shared-directory-name*`/jp1imm/log`
  - `/`*shared-directory-name*`/jp1imm/log/imcf`

  Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	Normal termination
`4`	Invalid option
`8`	Server cannot be connected
`12`	Memory shortage occurred
`16`	Invalid permission
`20`	Error, such as a file error or invalid path
`21`	Upper limit for number of concurrent executions reached
`24`	An input/output error occurred
`120`	System error occurred
`124`	Terminated due to other error

201 or greater	JavaVM start error occurred

Example

Import all the data of an export file located under the c:\temp:

```
jcfimport -i c:\temp
```

jcfmkcsdata

Function

This command creates from the host input information file (`host_input_data.csv`) and the Central Scope export file a Central Scope import file that contains monitoring tree information for a virtualization configuration. Alternatively, the command creates from the business group information file (`monitoring_system_data.csv`), the monitoring group information file (`monitoring_group_data.csv`), and the Central Scope export file a Central Scope import file to which the monitoring tree information of a business group is added.

For details about the business group information file (`monitoring_system_data.csv`) and the monitoring group information file (`monitoring_group_data.csv`), see *9.7.1(5) Business group information* and *9.7.1(6) Monitoring group information* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Format

```
jcfmkcsdata
          { -f host-input-information-file-name Central-Scope's-export-file
-name | -g business-group-information-file-name monitoring-group-information
-file-name Central-Scope's-export-file-name }
          -o export-file-name
          [-r]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-f` *host-input-information-file-name Central-Scope's-export-file-name*

Specifies the relative or absolute path of the host input information file (`host_input_data.csv`) exported by the `jcfexport` command and of the file exported by the `jcsdbexport` command. This option cannot be specified together with the `-g` option. If a path contains a space, enclose the entire path in double-quotation marks (`"`).

For the Central Scope's export file, specify the file to which a server-oriented tree has been exported.

For details about the host input information file (`host_input_data.csv`), see *9.7.1(1) Host information* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

`-g` *business-group-information-file-name monitoring-group-information-file-name Central-Scope's-export-file-name*

Specifies the business group information file exported by using the `jcfexport` command (`monitoring_system_data.csv`), the monitoring group information file (`monitoring_group_data.csv`), and the file exported by using the `jcsdbexport` command, expressed as a relative path or an absolute path. This option cannot be specified together with the `-f` option. If the path contains a space, enclose the entire path in double-quotation marks (").

For the Central Scope's export file, specify the file to which a server-oriented tree was exported. Note that for the export file, specify a file exported from the monitoring object DB whose data version is 0810 or later.

`-o` *export-file-name*

Specifies the relative or absolute path of the Central Scope import file that is to be output by the command. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (").

`[-r]`

This option sets whether to use the virtualization system configuration tree contained in the JP1/IM - Manager (Central Scope) export file specified by the argument. When this option is specified, the command creates a new file without using the virtualization system configuration tree contained in the JP1/IM - Manager (Central Scope) export file. If this option is not specified, a new virtualization system configuration tree is added to the virtualization system configuration tree contained in the JP1/IM - Manager (Central Scope) export file.

Return values

`0`	Normal termination
`1`	Argument error
`2`	Specified file is invalid
`3`	Specified input file was not found
`4`	Export file already exists
`5`	No permission to access a specified file
`6`	Insufficient memory
`7`	An input/output error occurred
`9`	Insufficient disk space
`10`	Execution permission error
`11`	Forced termination by pressing the **Ctrl** and **C** keys
`12`	The data version of the specified Central Scope export file is old
`20`	A reserved device was specified for the file path
`99`	Other error
`122`	Command was not executed from the administrator console (Windows only)

jcfmkhostsdata

Function

This command uses a virtualization configuration information file to update a host input information file.

Format

```
jcfmkhostsdata
          -imcf host-input-information-file
          -vm virtualization-configuration-information-file
          -o output-file-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-imcf` *host-input-information-file*

Specifies the relative or absolute path name of the host input information file. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-vm` *virtualization-configuration-information-file*

Specifies the relative or absolute path name of the virtualization configuration information file. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-o` *output-file-name*

Specifies the relative or absolute path name of the host input information file to which the result of updating the host input information file is to be output. This option is mandatory. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

Return values

`0`	Normal termination
`1`	Argument error
`2`	Insufficient memory
`3`	JavaVM start error occurred
`4`	Execution permission error (Windows only)
`5`	Command was not executed from the administrator console (Windows only)

6	Output file already exists
7	A specified file is invalid
8	A specified input file was not found
9	No permission to access a specified file
10	An input/output error occurred
99	Other error

jcfthreaddmp (Windows only)

Function

This command creates a Java thread dump of IM Configuration Management - View.

Execute this command to collect a Java thread dump under the following circumstances:

- Window operation has become disabled.
- There are no stopped IM Configuration Management - View processes or IM Configuration Management server processes.

The command outputs a Java thread dump of IM Configuration Management - View to a text file in the `log` directory:

`%ALLUSERSPROFILE%\Hitachi\JP1\JP1_DEFAULT\JP1CoView\log`

If you create a thread dump of IM Configuration Management - View while it is running normally, JavaVM will become unstable, in which case you will have to restart IM Configuration Management - View.

Format

```
jcfthreaddmp process-ID
```

Execution permission

None (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

View-path`\bin\`

Arguments

process-ID

Specifies the process ID of the `java.exe` process of IM Configuration Management - View that has become disabled.

The number of binds that can be specified by the process ID depends on OS limitations.

`CTRL_BREAK_EVENT` is not sent to a process other than IM Configuration Management - View (`java.exe`).

Return values

`0`	Normal termination
`1`	Open error or argument error
`2`	Process check error
`3`	Thread dump output request transmission error
`4`	Execution permission error
`10`	Other error

Example 1

The process ID of the IM Configuration Management - View that is disabled is 1234:

```
jcfthreaddmp 1234
```

Example 2

Identify the process ID of the java.exe process that corresponds to the IM Configuration Management - View:

Use the procedure below to identify the process ID of the java.exe process that corresponds to the disabled IM Configuration Management - View and then specify that process ID in the jcfthreaddmp command.

If you are running multiple instances of IM Configuration Management - View, there are also multiple java.exe processes. In such a case, you use the procedure described below to identify the process ID.

1. Add a **PID (Process Identifier)** column.

   Open Task Manager's **Process** page, from the **View** menu choose **Select Columns**, and then select the **PID (Process Identifier)** check box in the Select Columns dialog box.

2. Check whether the relevant IM Configuration Management - View instance is disabled.

   On the Task Manager's **Applications** page, select IM Configuration Management - View. From the right-click pop-up menu, choose **Bring to Front**. Check if the IM Configuration Management - View displayed in front is disabled.

3. Display the PID (process identifier) of the java.exe process that corresponds to the disabled IM Configuration Management - View.

   On the **Applications** page, select the disabled IM Configuration Management - View, and then from the right-click pop-up menu, choose **Go To Process**.

   The **Processes** page is displayed and the java.exe line of the disabled IM Configuration Management - View is selected. The PID column of that line is the process ID of the java.exe process that corresponds to the disabled IM Configuration Management - View.

jddcreatetree

Function

This command collects system configuration information from products managed by the Intelligent Integrated Management server to create the IM management node-related files, which in turn are input to the `jddupdatetree` command. Before you can execute this command, you must execute the `jddsetaccessuser` command to set a user ID and password that are required for authentication.

For details about the `jddupdatetree` and `jddsetaccessuser` commands, see *jddupdatetree* and *jddsetaccessuser* in *Chapter 1. Commands*.

This command requests the Intelligent Integrated Management Base to create the IM management node-related files and waits until the request is completed.

Before you can execute this command, you must complete definitions in the following files:
system node definition file (`imdd_systemnode.conf`), category name definition file for IM management nodes (`imdd_category_name.conf`), and target host definition file for configuration collection (`imdd_target_host.conf`). Additionally, you must complete the host name definition file (`imdd_host_name.conf`) for mapping between aliases and real host names if you want IM management nodes to include products that can have aliases for host names.

For details about the IM management node-related files, see the section that describes the IM management node-related files in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the definition files, see *System node definition file (imdd_systemnode.conf)*, *Category name definition file for IM management nodes (imdd_category_name.conf)*, *Target host definition file for configuration collection (imdd_target_host.conf)*, and *Host name definition file (imdd_host_name.conf)* in *Chapter 2. Definition Files*.

Format

```
jddcreatetree -o directory-name [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-o` *directory-name*

Specifies the path of the directory that stores files to be created. The value can be an absolute path or a relative path from the directory where this command is executed. The value must be enclosed in double quotation marks (`"`) if a space is included. The length of the path can be up to 200 characters.

`-h` *logical-host-name*

Specifies the logical host name of JP1/IM if JP1/IM is running in a cluster system.

If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

The length of *logical-host-name* must be equal to or less than 32 bytes to successfully collect the configuration information of the logical host. Otherwise, the `jddcreatetree` command fails with the message KAJY02015-E and the configuration management tree will not be updated.

Notes

- You cannot execute the `jddcreatetree` command concurrently multiple times. Doing so results in an error.
- While the `jddupdatetree` command and `jddupdatesuggestion` command are running, you cannot execute the `jddcreatetree` command . Doing so results in an error.
- Before you can execute the `jddcreatetree` command, JP1/IM - Manager and the IM database must be running.
- To use `jddcreatetree` command with integrated manager hosts, the intelligent integrated management base service and the JP1/IM agent management base services of the base or relay manager hosts must be running.
- Do not stop JP1/IM - Manager or the IM database while the `jddcreatetree` command is running.
- If you have defined the base manager or the relay manager, verify if the system hierarchy has been synchronized, and then execute the `jddcreatetree` command on the integrated manager. When on site manager and relay manager, there is no need to execute the `jddcreatetree` command.
- Execute the `jddcreatetree` command during a period when no job is running on the JP1/AJS3 - Manager host. Otherwise, each processing might be delayed as both processing loads are required simultaneously.
- Execute the `jddcreatetree` command when the JP1/AJS3 - Manager service is running. If the `jddcreatetree` command is executed when the JP1/AJS3 - Manager service is stopped or in the process of starting or stopping, the information collection fails.
- Do not stop the JP1/AJS3 service from which information is collected when the `jddcreatetree` command is collecting information. Doing so might delay the stop processing of the service.
- The `jddcreatetree` command cannot collect the unit definition information that includes multi-byte characters other than Japanese. If such information is collected, the configuration management tree might not be displayed correctly.
- The information collection might fail if control characters are included in the information that the `jddcreatetree` command collects, such as unit names, unit definition information, execution agent names, and JP1 resource group names. Do not include control characters in the information to be collected.
- If JP1/PFM is a linked product for configuration collection, in the target host definition file for configuration collection (`imdd_target_host.conf`), set the definition so that JP1/PFM is first (at the top of the file), and then execute the `jddcreatetree` command.
- If the `jddcreatetree` command is executed according to a method different from the above, a failure might occur.

- If JP1/OA is a linked product for configuration collection, collect the configuration information for JP1/OA separately from collecting configuration for other products.
- If the `jddcreatetree` command is executed according to a method different from the following, a failure might occur.
  1. In the target host definition file for configuration collection (`imdd_target_host.conf`), set the definition for linked products other than JP1/OA.

     At this time, if JP1/PFM is to be included in the targets for configuration collection, set the definition so that JP1/PFM is first (at the top of the file).
  2. Execute the `jddcreatetree` command.
  3. In the target host definition file for configuration collection (`imdd_target_host.conf`), set the definition for JP1/OA.
  4. Use the "`-o`" option to specify the same directory name as in step 2, then execute the `jddcreatetree` command.

Return values

0	Normal termination
1	Normal termination (invalid property)
2	Exclusive locked
3	Invalid argument
4	Invalid logical host name
5	Authentication information used by the Intelligent Integrated Management Base is not set
6	Missing information required for the `jddcreatetree` command to run
7	No execution permission for the `jddcreatetree` command
8	The specified directory is not accessible
9	The path to the specified directory is too long
11	Failed to connect to the Intelligent Integrated Management Base
12	The Intelligent Integrated Management Base could not be authenticated
13	A required file does not exist
14	A required file could not be read
15	A required file has an invalid format
16	A required file has an invalid description
17	Information could not be received from the plug-in
18	Invalid information was received from the plug-in
20	The IM management node file could not be created
21	The IM management node link file could not be created
23	The IM management node tree file could not be created
26	The user used for authentication has insufficient permissions
255	System error

Example 1

Specify that created files will be stored in `C:\tmp`:

```
$ jddcreatetree -o C:\tmp
KAJY02009-I The command (jddcreatetree) has started.
KAJY02010-I The command (jddcreatetree) terminates normally.
```

Example 2

Specify that created files will be stored in `C:\tmp` and specify a logical host named `ronri`:

```
$ jddcreatetree -o C:\tmp -h ronri
KAJY02009-I The command (jddcreatetree) has started.
KAJY02010-I The command (jddcreatetree) terminates normally.
```

jddupdatetree

Function

Based on the IM management node-related files acquired with the `jddcreatetree` command and the IM management node link definition file (`imdd_nodeLink_def.conf`) defined manually by the user, this command creates information regarding both the IM management node tree and the link between IM management nodes, and evaluates configuration information.

You can specify one of the following two options to designate how you want the system configuration information to be applied. The status of IM management nodes is evaluated differently depending on which option is specified.

If you specify the new and rebuilding mode as a way to apply system configuration information, this command acquires all the JP1 events stored in the integrated monitoring database and evaluates the status of each IM management node. If you specify the configuration change mode as a way to apply system configuration information, the command directly inherits and evaluates information regarding both existing JP1 events and mapping between those JP1 events and IM management nodes, instead of reacquiring all the JP1 events stored in the integrated monitoring database.

Specify the *new and rebuilding mode* in the following cases:

- When you create a new configuration
- When you correct any misconfiguration
- When you backed up the IM database (`jimdbbackup` command) and then recovered it (`jimdbrecover` command)
- When you unset up the integrated monitoring database (`jcodbunsetup` command) and set it up again (`jcodbsetup` command)
- When the intelligent integrated management database is backed up (execute `jimgndbbackup` command) and recovered (execute `jimgndbrestore` command)
- When you upgraded JP1/IM - Manager in the environment where the Intelligent Integrated Management Base was used

Specify the *configuration change mode* in the following case:

- When a managed target of the Intelligent Integrated Management Base is added, removed, or modified in addition to correction of misconfiguration

For details about how to apply system configuration information, see *3.5.7 Modes of applying system configuration information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Before executing this command, execute the `jddsetaccessuser` command to set the user ID and password information required for authentication.

For details about the `jddcreatetree` command, see *jddcreatetree* in *Chapter 1. Commands*.

This command requests the Intelligent Integrated Management Base to apply the IM management node-related files and waits until the request is completed.

Format

```
jddupdatetree -i directory-name [{-r|-c}] [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-i` *directory-name*

Specifies the path of the directory that stores files created by the `jddcreatetree` command. The value can be an absolute path or a relative path from the directory where this command is executed. The value must be enclosed in double quotation marks (`"`) if a space is included.

`-r|-c`

Specifies an option that determines how system configuration information will be applied.

`-r`

Specify this option when you want to apply system configuration information in the new and rebuilding mode. You cannot specify this option along with the `-c` option. In this mode, system configuration information is applied in almost the same manner as in version 12-10 or earlier.

`-c`

Specify this option when you want to apply system configuration information in configuration change mode. You cannot specify this option along with the `-r` option.

`-h` *logical-host-name*

Specifies the logical host name of JP1/IM if JP1/IM is running in a cluster system.

If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Notes

- You cannot execute the `jddupdatetree` command concurrently multiple times. Doing so results in an error.
- While the `jddupdatetree` command and `jddupdatesuggestion` commans are running, you cannot execute the `jddcreatetree` command. Doing so results in an error.
- Before you can execute the `jddupdatetree` command, JP1/IM - Manager and the IM database must be running.
- Do not stop JP1/IM - Manager or the IM database while the `jddupdatetree` command is running.
- When neither the `-r` option nor the `-c` option is specified, system configuration information is applied according to the setting specified for the `jp1.imdd.simt.updateMode` property in the Intelligent Integrated Management Base definition file (`imdd.properties`).

When you newly install JP1/IM - Manager, `change` (configuration change mode) is set for this property. When you upgrade from version 12-10 or earlier, nothing is defined for this property. In this case, it is assumed that `reconfigure` (new and rebuilding mode) is set. We advise you to change this setting to suit your operational needs.

- If a registered JP1 event is included while the host mapping function for the problem source in the integrated monitoring DB is disabled, mapping between the JP1 event and the IM management node might fail, and the warning message KAJY02022-W might be output. For details regarding mapping between a JP1 event and an IM management node, see *3.9.1 Evaluations using JP1 events* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Return values

0	Normal termination
1	Normal termination (invalid property)
2	Exclusive locked
3	Invalid argument
4	Invalid logical host name
5	Authentication information used by the Intelligent Integrated Management Base is not set
6	Missing information required for the `jddupdatetree` command to run
7	No execution permission for the `jddupdatetree` command
8	The specified directory does not exist
10	IM database service is not running
11	Failed to connect to the Intelligent Integrated Management Base
12	The Intelligent Integrated Management Base could not be authenticated
13	A required file does not exist
14	A required file could not be read
15	A required file has an invalid format
16	A required file has an invalid description
17	Event information could not be received
19	Information could not be received from the plug-in
22	Master file alternate failed
26	The user used for authentication has insufficient permissions
27	There are suggestion definitions that are not mapped to any of the IM management nodes
28	Failed to create suggestion-related master files#
29	Failed to replace the suggestion-related master files#
255	System error

#
These files collectively refer to master information related to suggestions (including the suggestion definition master file, etc.). They are loaded when the JP1/IM - Manager service starts.

Example 1

Specify that files created by the `jddcreatetree` command are stored in `C:\tmp`:

```
$ jddupdatetree -i C:\tmp
KAJY02009-I The command (jddupdatetree) has started.
KAJY02010-I The command (jddupdatetree) terminates normally.
```

Example 2

Specify that files created by the `jddcreatetree` command are stored in `C:\tmp` and specify a logical host named `ronri`:

```
$ jddupdatetree -i C:\tmp -h ronri
KAJY02009-I The command (jddupdatetree) has started.
KAJY02010-I The command (jddupdatetree) terminates normally.
```

Example 3

Execute the command with the new and rebuilding mode specified as a way to apply system configuration information:

```
$ jddupdatetree -i C:\tmp -r
KAJY02009-I The command (jddcreatetree) has started.
KAJY02010-I The command (jddcreatetree) terminate normally.
```

Example 4

Execute the command with the configuration change mode specified as a way to apply system configuration information:

```
$ jddupdatetree -i C:\tmp -c
KAJY02009-I The command (jddcreatetree) has started.
KAJY02010-I The command (jddcreatetree) terminates normally.
```

jddsetaccessuser

Function

This command executes definitions related to the authentication of the Intelligent Integrated Management Base. The user ID and password defined with this command are used for authentication under the following circumstances:

- When connecting to a monitored JP1 product from the Intelligent Integrated Management Base
- When connecting to the Intelligent Integrated Management Base by using one of the commands provided by the Intelligent Integrated Management Base
- Authentication of the Intelligent Integrated Management Base when OpenID authentication linkage is enabled

Format

```
jddsetaccessuser -id user-ID -pw password [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-id` *user-ID*

Specifies a user ID of user who has administrator permissions for JP1/IM, JP1/PFM, and JP1/AJS.

The user ID must be a character string of 1 to 31 bytes.

Acceptable characters are alphanumeric characters and the following symbols: exclamation mark (`!`), dollar sign (`$`), percent sign (`%`), ampersand (`&`), underscore (_), hyphen (`-`), hash mark (`#`), and at mark (`@`).

Specified uppercase characters are handled as lowercase.

`-pw` *password*

Specifies a password for the user who you specified with the `-id` option.

The password must be a character string of 6 to 32 bytes.

Acceptable characters are alphanumeric characters and the following symbols: exclamation mark (`!`), hash mark (`#`), dollar sign (`$`), percent sign (`%`), ampersand (`&`), underscore (_), hyphen (`-`), asterisk (`*`), forward slash (`/`), single quotation mark (`'`), caret (^), left square bracket (`[`), right square bracket (`]`), left curly bracket (`{`), right curly bracket (`}`), left parenthesis (`(`), right parenthesis (`)`), semicolon (`;`), vertical bar (`|`), equal sign (=), plus sign (+), question mark (`?`), left angle bracket (<), and right angle bracket (>).

A password is case sensitive. A password must be enclosed in double quotation marks (`"`) if any of the following symbols is included: caret (^), left angle bracket (<), right angle bracket (>), vertical bar (`|`), and ampersand (`&`).

`-h` *logical-host-name*

Specifies the logical host name if you operate JP1/IM in a cluster system. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Return values

0	Normal termination
1	Invalid argument
2	A specified argument value was invalid
3	The file could not be created
4	Invalid logical host name
7	No execution permission for the `jddsetaccessuser` command
255	System error

Example 1

Specify a password of `ABCDEF` for the user `UserA`:

```
$ jddsetaccessuser -id UserA -pw ABCDEF
KAJY02009-I The command (jddsetaccessuser) has started.
KAJY02010-I The command (jddsetaccessuser) terminates normally.
```

Example 2

Specify a password of `ABCDEF` for the user `UserA` on the logical host `ronri`:

```
$ jddsetaccessuser -id UserA -pw ABCDEF -h ronri
KAJY02009-I The command (jddsetaccessuser) has started.
KAJY02010-I The command (jddsetaccessuser) terminates normally.
```

jddsetproxyuser

Function

This command sets authentication information for the proxy server when REST APIs are executed from plug-ins that are provided by JP1/IM - Manager (Intelligent Integrated Management Base). This setting is not needed if you do not use proxy server authentication.

Format 1

```
Usage:
jddsetproxyuser {-list|-add -id user-ID -pw password |-rm -id user-ID} [-h l
ogical-host-name]
```

Format 2

```
jddsetproxyuser -list [-h logical-host-name]
```

Format 3

```
jddsetproxyuser -add -id user-ID -pw password [-h logical-host-name]
```

Format 4

```
jddsetproxyuser -rm -id user-ID [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-list`

Specify this option if you get authentication information for the proxy server configured in the Intelligent Integrated Management Base.

`-add`

Specify this option if you update the authentication information for the proxy server configured in the Intelligent Integrated Management Base. If this option is specified, the `-id` option and `-pw` option must be specified. If they are omitted, an error occurs.

`-rm`

Specify this option if you remove the authentication information for the proxy server configured in the Intelligent Integrated Management Base. If this option is specified, the `-id` option must be specified. If it is omitted, an error occurs.

`-id` *user-ID*

Specifies the user ID of a user for proxy server authentication.

`-pw` *password*

Specifies the password for the user you specified with the `-id` option.

`-h` *logical-host-name*

Specifies the logical host name of JP1/IM if JP1/IM is running in a cluster system.

If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Notes

- You cannot execute the jddsetproxyuser command concurrently multiple times. Doing so results in an error.
- Do not stop JP1/IM - Manager or the IM database while the jddsetproxyuser command is running.
- You cannot execute the `jddsetproxyuser` command together with the API for setting proxy authentication information. For details about the proxy credential setup API, see *5.9.1 Proxy credential setup*.
- If the `jddsetproxyuser` command is executed while JP1/IM - Manager is not running, the `KAJY52015-W` message is output and the setting will take effect next time JP1/IM - Manager is started.

Return values

0	Normal termination
1	Invalid argument
2	Exclusive locked
3	A specified argument value was invalid
4	Invalid logical host name
5	Authentication information used by the Intelligent Integrated Management Base is not set
7	No execution permission for the jddsetproxyuser command
11	Failed to connect to the Intelligent Integrated Management Base
12	The Intelligent Integrated Management Base could not be authenticated
13	Update of proxy authentication information failed
255	System error

Example 1

The following is an example of getting authentication information for the proxy server configured in the Intelligent Integrated Management Base:

```
jddsetproxyuser -list
KAJY02009-I The command (jddsetproxyuser) has started.
User1
```

```
User2
KAJY02010-I The command (jddsetproxyuser) terminates normally.
```

Example 2

The following is an example of updating authentication information for the proxy server configured in the Intelligent Integrated Management Base:

```
jddsetproxyuser -add -id User3 -pw PASSWORD
KAJY02009-I The command (jddsetproxyuser) has started.
KAJY02010-I The command (jddsetproxyuser) terminates normally.

jddsetproxyuser -list
KAJY02009-I The command (jddsetproxyuser) has started.
User1
User2
User3
KAJY02010-I The command (jddsetproxyuser) terminates normally.
```

Example 3

The following is an example of removing authentication information for the proxy server configured in the Intelligent Integrated Management Base:

```
jddsetproxyuser -rm -id User3
KAJY02009-I The command (jddsetproxyuser) has started.
KAJY02010-I The command (jddsetproxyuser) terminates normally.

jddsetproxyuser -list
KAJY02009-I The command (jddsetproxyuser) has started.
User1
User2
KAJY02010-I The command (jddsetproxyuser) terminates normally.
```

jddupdatesuggestion

Function

This command loads all suggestion definition files located under the specified directory and applies them to the Intelligent Integrated Management Base.

When the suggestion definition files have already been applied to the Intelligent Integrated Management Base, the command discards all the definitions that have been applied and replaces them with the definitions provided in the specified suggestion definition files. When there is a mistake in one of the definitions provided in the suggestion definition files, the command suspends its processing the moment the mistake is found.

Before executing this command, execute the `jddsetaccessuser` command to set the user ID and password necessary for authentication.

Format

```
jddupdatesuggestion -i directory-name [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-i` *directory-name*

Specify either the absolute path to the directory under which the suggestion definition files are saved or the relative path to the same directory from the location where this command is executed. If the path name contains a space, enclose the entire path name in double quotation marks (`"`).

`-h` *logical-host-name*

Specify the logical host name when JP1/IM is running in a cluster system. When you omit this option, the command assumes that the logical host name specified in the `JP1_HOSTNAME` environment variable is set. When the `JP1_HOSTNAME` environment variable is not specified, the command assumes that the physical host name is set.

Notes

- You cannot execute multiple `jddupdatesuggestion` commands at a time. Doing so results in an error.
- You cannot execute this command while the `jddcreatetree` command or the `jddupdatetree` command is being executed. Doing so results in an error.

- You have to execute the `jddupdatesuggestion` command while the JP1/IM - Manager service is up and running.

Return values

0	Normal termination
1	Normal termination (with a warning message)
2	Concurrent execution error
3	Invalid argument
4	Invalid logical host name
5	Authentication information used by the Intelligent Integrated Management Base is not set
6	No execution permission for the `jddupdatesuggestion` command assigned
7	The specified directory does not exist
8	Failed to connect to the Intelligent Integrated Management Base
9	The Intelligent Integrated Management Base could not be authenticated
10	The user used for authentication has insufficient permissions
11	The suggestion definition files do not exist
12	Failed to load the suggestion definition files
13	The suggestion definition files have an invalid format
14	The suggestion definition files have an invalid description
15	Failed to create a suggestion definition master file#
255	System error

#

This refers to a single file to which information contained in the suggestion definition files specified with the `-i` option is output. This file serves as master information.

Example 1

Specify `C:\tmp` as the location to which to store the suggestion definition files:

```
$ jddupdatesuggestion -i C:\tmp
KAJY02009-I The command (jddupdatesuggestion) has started.
KAJY02010-I The command (jddupdatesuggestion) terminates normally.
```

Example 2

Specify `C:\tmp` as the location to which to store the suggestion definition files and `ronri` as the logical host:

```
$ jddupdatesuggestion -i C:\tmp -h ronri
KAJY02009-I The command (jddupdatesuggestion) has started.
KAJY02010-I The command (jddupdatesuggestion) terminates normally.
```

jddsetopinfo

Function

This command takes the Intelligent Integrated Management Base client information (client IDs and client secrets) registered with the OpenID provider for OpenID authentication linkage, and sets it in JP1/IM - Manager (Intelligent Integrated Management Base).

The client IDs and client secrets are used to authenticate the Intelligent Integrated Management Base clients registered with the OpenID provider. In order for this to work, this command must be executed prior to starting JP1/IM - Manager (Intelligent Integrated Management Base).

Format 1

```
Usage:
jddsetopinfo {-list|-add -provider OpenID-provider-name -id client-ID -secre
t client-secret|-rm -provider OpenID-provider-name} [-h logical-host-name]
```

Format 2

```
jddsetopinfo -list [-h logical-host-name]
```

Format 3

```
jddsetopinfo -add -provider OpenID-provider-name -id client-ID -secret clien
t-secret [-h logical-host-name]
```

Format 4

```
jddsetopinfo -rm -provider OpenID-provider-name [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path\bin\imdd\

In UNIX:

/opt/jp1imm/bin/imdd/

Arguments

-list

Specify this option to collect the client information registered with OpenID providers that is set in the Intelligent Integrated Management Base.

The only option you can specify along with this option is the `-h` option.

`-add`

Specify this option to add the client information registered with OpenID providers to the Intelligent Integrated Management Base or update such client information that is set in the Intelligent Integrated Management Base. If you specify this option, the specification of the `-provider`, `-id`, and `-secret` options is mandatory. Without these options specified, the error message `KAJY02011-E` is output. This option cannot be specified along with any other options.

`-rm`

Specify this option to delete the client information registered with OpenID providers from the Intelligent Integrated Management Base. If you specify this option, the specification of the `-provider` option is mandatory. Without this option specified, the error message `KAJY02011-E` is output.

This option cannot be specified along with options other than the `-provider` and `-h` options.

`-provider` *OpenID-provider*

Specify the OpenID provider name. The value you specify here must be the <*key-name-of-the-OpenID-provider*> that you have set as an OpenID provider definition inside the Intelligent Integrated Management Base definition file (`imdd.properties`). For details, see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files*.

This option cannot be specified along with the `-list` option.

`-id` *client-ID*

Specify the client ID. The characters you specify here must conform to the specifications set out by the applicable OpenID provider.

This option cannot be specified along with options other than the `-list` and `-rm` options.

`-secret` *client-secret*

Specify the client secret for the client ID specified with the `-id` option. The characters you specify here must conform to the specifications set out by the applicable OpenID provider.

This option cannot be specified along with options other than the `-list` and `-rm` options.

`-h` *logical-host-name*

Specify the logical host name when JP1/IM is running in a cluster system. When you omit this option, the command assumes that the logical host name specified in the `JP1_HOSTNAME` environment variable is set. When the `JP1_HOSTNAME` environment variable is not specified, the command assumes that the physical host name is set.

Notes

- You cannot execute multiple `jddsetopinfo` commands at a time. Doing so results in an error.
- You have to execute the `jddsetopinfo` command before starting JP1/IM - Manager (Intelligent Integrated Management Base).
- If you execute the `jddsetopinfo` command while JP1/IM - Manager (Intelligent Integrated Management Base) is up and running, the settings are applied the next time you start JP1/IM - Manager (Intelligent Integrated Management Base).

Return values

0	Normal termination
2	Failed to establish exclusive control
3	Invalid argument

4	Invalid logical host name
5	Failed to specify the setting
6	The specified OpenID provider's client information does not exist
7	No execution permission for the `jddsetopinfo` command
255	System error

Example 1

Collect the client information registered with OpenID providers that is set in the Intelligent Integrated Management Base:

```
jddsetopinfo -list
KAJY02009-I The command (jddsetopinfo) has started.
okta:IM1210
keycloak:IM1210
KAJY02010-I The command (jddsetopinfo) terminates normally.
```

Example 2

Add the client information registered with the OpenID provider to the Intelligent Integrated Management Base or update such information that is set in the Intelligent Integrated Management Base:

```
jddsetopinfo -add -provider okta -id id001 -secret SECRET
KAJY02009-I The command (jddsetopinfo) has started.
KAJY02010-I The command (jddsetopinfo) terminates normally.
```

Check the current status.

```
jddsetopinfo -list
KAJY02009-I The command (jddsetopinfo) has started.
okta:id001
keycloak:id001
KAJY02010-I The command (jddsetopinfo) terminates normally.
```

Example 3

Delete the client information registered with the OpenID provider from the Intelligent Integrated Management Base:

```
jddsetopinfo -rm -provider okta
KAJY02009-I The command (jddsetopinfo) has started.
KAJY02010-I The command (jddsetopinfo) terminates normally.
```

Check the current status.

```
jddsetopinfo -list
KAJY02009-I The command (jddsetopinfo) has started.
keycloak:User2
KAJY02010-I The command (jddsetopinfo) terminates normally.
```

jddupdatessomap

Function

This command applies the mapping information defined in the single sign-on mapping definition file to JP1/IM - Manager (Intelligent Integrated Management Base).

Note that if this command is executed when the single sign-on mapping definition file has no valid property at all, the `KAJY52031-W` message is output and the applied single sign-on mapping definitions are cleared.

Format

```
Usage:
jddupdatessomap [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console.)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-h` *logical-host-name*

Specify the logical host name when JP1/IM is running in a cluster system. When you omit this option, the command assumes that the logical host name specified in the `JP1_HOSTNAME` environment variable is set. When the `JP1_HOSTNAME` environment variable is not specified, the command assumes that the physical host name is set.

Notes

- You cannot execute multiple `jddupdatessomap` commands at a time. Doing so results in an error.
- You have to execute the `jddupdatessomap` command while the Intelligent Integrated Management Base service is up and running.

Return values

0	Normal termination
1	Normal termination (invalid property or empty single sign-on mapping definition)
2	Failed to establish exclusive control
3	Invalid argument
4	Invalid logical host name

5	Authentication information used by the Intelligent Integrated Management Based is not set
7	No permission necessary to execute the command
11	Failed to connect to the Intelligent Integrated Management Base
12	The Intelligent Integrated Management Base could not be authenticated
13	Failed to apply information to the Intelligent Integrated Management Base
14	Definition file load error
255	System error

Example

```
jddsetssomap
KAJY02009-I The command (jddsetssomap) has started.
KAJY02010-I The command (jddsetssomap) terminates normally.
```

jddupdateaction

Function

This command loads a user-defined auto response action definition file and applies it to Intelligent Integrated Management Base.

Format

```
Usage:
jddupdateaction [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdd\`

In UNIX:

`/opt/jp1imm/bin/imdd/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is set empty string, the command assumes the physical host name,

If this option is omitted and the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Notes

- If you use this command, JP1/IM3-Manager service must be running.

Return values

0	Normal termination
1	Normal termination (with a warning message)
2	Invalid option
3	Invalid logical host name
4	Authentication data used by Intelligent Integrated Management Base has not been setup.
5	No execution permission for the command
6	Failed to connect to the Intelligent Integrated Management Base

7	Failed to be authenticated to the Intelligent Integrated Management Base
8	The user used for authentication has insufficient permissions
9	Failed to load the auto response action definition file
10	Incorrect format of the auto response action definition file
11	Incorrect content of the auto response action definition file
255	System error occurred

Example

The following shows an example in which the logical host is set to "ronri".

```
$ jddupdateaction -h ronri
KAJY02009-I The command (jddupdateaction) has started.
KAJY02010-I The command (jddupdateaction) terminates normally.
```

jcfview (Windows only)

Function

This command starts IM Configuration Management - View. If the `-h`, `-u`, and `-p` options are specified, the command logs in to IM Configuration Management - View automatically without displaying the Login window.

Format

```
jcfview [-h connection-target-host-name] [-u user-name] [-p password]
```

Execution permission

None

Storage directory

View-path`\bin\`

Arguments

`-h` *connection-target-host-name*

Specifies the name of the host where the IM Configuration Management to be logged into is running. For the host name, from 1 to 255 bytes of characters are permitted. You can specify only a host where JP1/IM - Manager is running.

For the connection-target host name, you can specify the following:

- Host name defined on the host where the command is used
- Host name whose address can be resolved on the host where the command is used
- IP address

  Only addresses in IPv4 address format can be specified as IP address. Addresses in IPv6 address format cannot be specified.

This option is optional. However, if you specify the `-p` option, you must specify this option.

If you start IM Configuration Management - View by specifying only the `-h` option or both the `-h` and the `-u` options, the Login window is displayed by using these arguments as the default values. If only the `-h` and `-p` options are specified to start IM Configuration Management - View, an error results.

`-u` *user-name*

Specifies a JP1 user name that has been registered in the authentication server. For the JP1 user name, from 1 to 31 alphanumeric characters are permitted (for alphabetic characters, only lowercase letters are permitted).

This option is optional. However, if you specify the `-p` option, you must specify this option.

If you start IM Configuration Management - View by specifying only the `-u` option or both the `-h` and the `-u` options, the Login window is displayed by using these arguments as the default values. If only the `-u` and `-p` options are specified to start IM Configuration Management - View, an error results.

`-p` *password*

Specifies the password for the specified user name. For the password, from 6 to 32 alphanumeric characters are permitted. Alphabetic characters are case sensitive. This option is optional.

If you specify this option, you must also specify the `-h` and `-u` options.

Return values

0	Normal termination
1	Argument error
2	Insufficient memory
3	Resource acquisition failed
4	Error message creation failed
5	Forced termination of IM Configuration Management - View
255	System error

Example 1

Start IM Configuration Management - View and display the Login window:

```
jcfview
```

Example 2

Enable automatic login without displaying the Login window:

This example specifies the connection-target host (host1), user name (user2), and password (password) to start IM Configuration Management - View:

```
jcfview -h host1 -u user2 -p password
```

jcfvirtualchstat

Function

Updates the virtualization configuration of the specified host.

If the virtualization configuration managed by the virtualization environment management software is changed, the change can be applied to IM Configuration Management by executing this command.

Note that a maximum of five commands can be executed concurrently.

Format

```
jcfvirtualchstat    -c host-name
                    [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imcf\`

In UNIX:

`/opt/jp1imm/bin/imcf/`

Arguments

`-c` *host-name*

Specifies the name of the host whose virtualization configuration information is to be collected. For the host name, specify a maximum of 255 characters.

`-h` *logical-host-name*

For operation in a cluster system, this option specifies the logical host name. Specify the name of a logical host with a maximum of 255 bytes. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1imm`

- /*shared-directory-name*/jp1imm/log
- /*shared-directory-name*/jp1imm/log/imcf

Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

0	Normal termination
4	Invalid option
8	Unable to connect to the server
12	Insufficient memory
16	Invalid permission
21	Upper limit for number of concurrent executions reached
24	Input/output error
120	System error occurred
124	Termination due to an error not listed here
201 or greater	JavaVM start error occurred

jco_killall.cluster (UNIX only)

Function

When you are operating in a cluster system, this command forcibly terminates the JP1/IM - Manager processes.

Executing the `jco_stop.cluster` command during cluster operation may not stop all processes, resulting in a cluster operation failure. The `jco_killall.cluster` command forcibly terminates processes. Use this command only when processes cannot be terminated by the normal method of stopping JP1/IM - Manager Service.

The command can terminate the following processes:

- Process management (`jco_spmd`)
- Automatic Action Service (`jcamain`)
- Event Console Service (`evtcon`)
- Event Base Service (`evflow`)
- Event Generation Service (`evgen`)
- Central Scope Service (`jcsmain`)
- IM Configuration Management Service (`jcfmain`)
- IM database service
- Intelligent Integrated Management database service
- Trend Data Management Service
- Intelligent Integrated Management Base Service (`jddmain`)
- Servicing JP1/IM agent management base (`imbase)`
- Servicing JP1/IM agent management base (`imbaseproxy`)

Format

```
jco_killall.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1cons/`

Arguments

logical-host-name

Specifies a logical host name set in JP1/Base. You can specify 1 to 32 bytes of characters. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Notes

This command checks the first 32 bytes of the logical host name, and then forcibly terminates the corresponding process. The command cannot forcibly terminate a process on a logical host whose name consists of 33 bytes or more.

Return values

`0`	Normal termination
`1`	Logical host name is not specified
`2`	There is no log directory

jco_spmd_reload

Function

This command updates the status of JP1/IM - Manager processes. When you have changed the definition information for JP1/IM - Manager, you must reload the new information to enable it.

The `jco_spmd_reload` command enables the information in the definition files listed below. For details, see *When the definitions are applied* for each definition file in *Chapter 2. Definition Files*.

- The following information is located in the automated action environment definition file (`action.conf.update`):
  - AND event storage period (`EVENTALIVEPERIOD`)
  - Default action executing user (`ACTIONEXECUSER`)
  - Automatic action issuance event (`SENDABLE_EVENT`)
  - Event-issuing host name acquisition method (`HOSTINEVENT`)
- Automatic action notification definition file (`actnotice.conf`)
- Extended startup process definition file (`jp1co_service.conf`)
- Health check definition file (`jcohc.conf`)
- Event guide information file (`jco_guide.txt`)
- Host information file (`jcs_hosts`)
- Guide information file (`jcs_guide_`*xxx*`.txt`)
- Correlation event generation system profile (`egs_system.conf`)
- Correlation event generation environment definition file
- Definition file for manually registering incidents (`incident.conf`)
- Configuration file for incident inheritance information (`incident_info.conf`)
- File that defines the event source host mapping `(user_hostmap.conf)`
- Severity changing definition file (`jcochsev.conf`)
- File that defines which items are displayed for severity changing definitions (`chsev_attr_list.conf`)
- File that defines automatic input of severity changing definitions (`chsev_auto_list.conf`)
- File that defines which items are displayed for event conditions `(attr_list.conf)`
- File that defines which items are displayed for repeated event conditions (`event_storm_attr_list.conf`)
- File that defines automatic input of repeated event conditions (`event_storm_auto_list.conf`)
- File that defines which items are displayed for common exclusion-conditions `(common_exclude_filter_attr_list.conf)`
- File that defines automatic input of common exclusion-conditions `(common_exclude_filter_auto_list.conf)`
- Definition file for extended event attributes
- Definition file for extended event attributes (extended file)
- Definition file for changed display messages (`jcochmsg.conf`)

- File that defines automatic input of display message change definitions (`chmsg_auto_list.conf`)
- File that defines which items are displayed for display message change definitions (`chmsg_attr_list.conf`)
- Definition file for opening monitor windows
- Apply-IM-configuration-method definition file (`jp1cf_applyconfig.conf`)

Format

```
jco_spmd_reload [-h logical-host-name]
                [-t monitoring-period]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The permitted length is from 1 to 255 bytes characters. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-t` *monitoring-period*

Specifies in seconds the amount of time to wait for the `jco_spmd_reload` command to terminate. The permitted value is from 0 to 32,767 (seconds). If the `jco_spmd_reload` command does not terminate within the specified amount of time, the system assumes that execution of the `jco_spmd_reload` command has failed. The default is 60 seconds.

Notes

- The jco_spmd_reload command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
Other than `0`	Abnormal termination

jco_spmd_status

Function

This command displays the startup status of the JP1/IM - Manager processes.

Format

```
jco_spmd_status [-h logical-host-name]
                [-t monitoring-period]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The permitted length is from 1 to 255 bytes characters. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-t` *monitoring-period*

Specifies in seconds the amount of time to wait for the `jco_spmd_status` command to terminate. The permitted value is from 0 to 32,767 (seconds). If the `jco_spmd_status` command does not terminate within the specified amount time, the system assumes that execution of the `jco_spmd_status` command has failed. The default is 60 seconds.

Return values

`0`	All child processes are running
`1`	• Error occurred during communication, such as in process management. • When you are operating in a cluster system, the shared folder (shared directory) is not mounted. • Execution permission error (Windows only).
`4`	Some child processes are running
`8`	All stopped
`12`	Request processing is underway (can be retried)

jco_start (UNIX only)

Function

This command is a script for starting JP1/IM - Manager automatically.

To execute this command, you must have performed the following procedure after you completed installation and setup of JP1/IM - Manager:

```
# cd /etc/opt/jp1cons
```

```
# cp -p jco_start.model jco_start
```

With these operations, JP1/IM - Manager starts automatically when the system starts. If you do not want JP1/IM - Manager to start automatically at the system startup, do not perform these operations.

You must perform these operations if you set JP1/IM - Manager version 10 or earlier to start automatically.

For details about configuring the automatic startup settings, see *2.18.2 Setting automatic startup and automatic stop (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

To start JP1/IM - Manager manually, execute the `/etc/opt/jp1cons/jco_start.model` script, or a file to which this script has been copied.

If you use a script to which `jco_start.model` has been copied in JP1/IM - Manager version 10 or earlier, overwrite it with `jco_start.model`.

Before you execute this command, make sure that JP1/Base is running. JP1/IM - Manager uses the functions of JP1/Base (prerequisite product).If this command is executed when the following all conditions are satisfied, the command starts the IM database service and then starts JP1/IM - Manager:

- The IM database service has been set up.
- The integrated monitoring database is used or IM Configuration Management Service is set to be started.

If you are using Intelligent Integrated Management Database, after starting IM Database services the above, further services start in the order of the Intelligent Integrated Management Database and Trend Data Management Service, and then start JP1/IM - Manager at the end.

The command terminates with a return value of 0 after issuing a startup request to the group of JP1/IM - Manager processes. To check whether the group of processes has started successfully, use the `jco_spmd_status` command after the `jco_start` command has terminated to display the process IDs of the services that have started. Note that the process ID of the IM database service is not displayed.

Format

```
jco_start
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1cons/`

Note

- If you want to execute this command as a remote shell command, disconnect standard input, standard output, and standard error output (assign `/dev/null` to standard input, standard output, and standard error output). Note that the remote shell command might not terminate even when processing for starting JP1/IM - Manager has finished.
- Execute this command in an environment in which the environment variable `JP1_HOSTNAME` has not been set. If you execute this command in an environment in which the environment variable `JP1_HOSTNAME` has been set, the command will attempt to start JP1/IM - Manager on the logical host set in the environment variable `JP1_HOSTNAME` rather than on the physical host. Because this command does not support logical hosts, you must delete the environment variable `JP1_HOSTNAME` if you want to start JP1/IM - Manager on the physical host.
- The jco_start command cannot be executed together with the `jco_spmd_status` command.

Return values

0	Normal termination
1	More than one argument is specified, the event service is not running, or the IM database service cannot be started
2	There is no log directory

Example 1

When the integrated monitoring database is used:

Input value:

```
jco_start
```

Result:

```
Please wait a minutes, now starting the IM database service...
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
Please wait a minutes, now starting JP1/IM - Manager...
KAVB3690-I Processing to report the status of JP1_CONS has started.
Display the running processes
process name  process ID
      evflow      18990
     jcamain      19036
      evtcon      19037
KAVB3691-I All the processes have started.
```

Example 2

When the integrated monitoring database is not used and IM Configuration Management Service has not started:

Input value:

```
jco_start
```

Result:

```
Please wait a minutes, now starting JP1/IM - Manager...
KAVB3690-I Processing to report the status of JP1_CONS has started.
```

```
Display the running processes
process name  process ID
       evflow      19237
      jcamain      19277
       evtcon      19278
KAVB3691-I All the processes have started.
```

Example 3

When the IM database is not used:

Input value:

```
jco_start
```

Result:

```
Please wait a minutes, now starting the IM database service...
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11109-E The IM database service is not set up.
Unable start JP1/IM - Manager.
```

Example 4

When the integrated monitoring database and the trend data management database are used:

Input value:

```
jco_start
```

Result:

```
Please wait a minutes, now starting the IM database service...
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
Please wait a minutes, now starting the Intelligent Integrated DB...
KNAN12055-I The Intelligent Integrated Management Database Service wil
l now start.
KNAN12057-I The trend data management service will now start.
KNAN12056-I The Intelligent Integrated Management Database Service star
ted normally.
KNAN12058-I The trend data management service started normally.
KNAN12044-I The processing to confirm the service operating status wil
l now start.
KNAN12047-I The Intelligent Integrated Management Database Service is r
unning.
KNAN12048-I The trend data management service is running.
KNAN12045-I The processing to confirm the service operating status ende
d normally.
Please wait a minutes, now starting JP1/IM - Manager...
KAVB3690-I Processing to report the status of JP1_CONS has started.
Display the running processes
process name  process ID
      evflow      26290
```

```
     jcamain      26374
      evtcon      26375
     jddmain      26291
KAVB3691-I All the processes have started.
```

jco_start.cluster (UNIX only)

Function

When you are operating in a cluster system, this command starts JP1/IM - Manager on the logical host.

If you register this command into the cluster software, JP1/IM - Manager starts.

Before you execute this command, start JP1/Base on the same logical host. An error results if this command is executed while the event service of JP1/Base is not running.

The command terminates with a return value of 0 after issuing a startup request to the group of JP1/IM - Manager processes. To check whether the group of processes has started successfully, use the `jco_spmd_status` command after the `jco_start.cluster` command has terminated.

If this command is executed when the following condition is satisfied, the command starts the IM database service, starts in the order of the intelligent integrated management database and the trend data management service, and then starts JP1/IM - Manager:

- IM database service startup conditions (all conditions must be met)

- You have set up IM database on your logical host.
- The integrated monitoring database on the logical host is enabled or IM Configuration Management Service is set to be started.

- Startup requirements for the intelligent integrated management database service and the trend data management service

- You have set up the intelligent integrated management database on the logical host.

To execute this command, you must have executed `jp1cc_setup_cluster` and `jp1cs_setup_cluster` after installing and setting up JP1/IM - Manager. For the IM database service, you must set up the cluster system for the IM database service. For details about setting up a cluster system, see *Chapter 8. Operation and Environment Configuration in a Cluster System (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jco_start.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1cons/`

Arguments

logical-host-name

When you are operating in a cluster system, this option specifies the name of the logical host where this command is to be executed. The permitted length is from 1 to 63 bytes characters. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Note

- If you want to execute this command as a remote shell command, disconnect standard input, standard output, and standard error output (assign `/dev/null` to standard input, standard output, and standard error output). Note that the remote shell command might not terminate even when processing for starting JP1/IM - Manager has finished.
- The jco_start_cluster command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
`1`	More than one argument is specified, the event service is not running, or the IM database service cannot be started
`2`	There is no log directory

jco_stop (UNIX only)

Function

This command is a script for terminating JP1/IM - Manager automatically.

```
# cd /etc/opt/jp1cons
```

```
# cp -p jco_stop.model jco_stop
```

Once the foregoing procedure has been executed, JP1/IM - Manager terminates automatically when the system terminates.

If the IM database service is running, the IM database service is stopped automatically after JP1/IM - Manager has terminated.

If you are using the intelligent integrated management database, after stopping the JP1/IM - Manager, terminate the trend data management service, then the intelligent integrated management database and finally terminate the IM database service.

If JP1/IM - Manager does not terminate, the command outputs the `KAVB8800-E` message to standard output.

If the IM database service does not terminate, the command outputs the `KAVB8801-E` message to standard output.

To stop JP1/IM - Manager manually, execute the `/etc/opt/jp1cons/jco_stop.model` script, or a file to which the script has been copied.

Format

```
jco_stop
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1cons/`

Note

- Execute this command in an environment in which the environment variable `JP1_HOSTNAME` has not been set. If you execute this command in an environment in which the environment variable `JP1_HOSTNAME` has been set, the command will attempt to stop JP1/IM - Manager on the logical host that is set in the environment variable `JP1_HOSTNAME` rather than on the physical host. Because this command does not support logical hosts, you must delete the environment variable `JP1_HOSTNAME` if you want to stop JP1/IM - Manager on the physical host.
- The jco_stop command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
`1`	More than one argument is specified or the termination request resulted in a timeout

Example 1

JP1/IM - Manager and the IM database service are running:

Input value:

```
jco_stop
```

Result:

```
KAVB3674-I Termination processing of JP1_CONS has started.
KAVB3675-I The stop command terminated normally.
KNAN11185-I Processing to stop the IM database service will now start.
KNAN11028-I Please wait.
KNAN11187-I The IM database service stopped normally.
KNAN11186-I Processing to stop the IM database service ended normally.
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
```

Example 2

JP1/IM - Manager is running and the IM database service is not running:

Input value:

```
jco_stop
```

Result:

```
KAVB3674-I Termination processing of JP1_CONS has started.
KAVB3675-I The stop command terminated normally.
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
```

Example 3

Neither JP1/IM - Manager nor the IM database service is running:

Input value:

```
jco_stop
```

Result:

```
KAVB3674-I Termination processing of JP1_CONS has started.
KAVB3662-I The process management is not running.
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
```

Example 4

JP1/IM - Manager is not running and the IM database service is running:

Input value:

```
jco_stop
```

Result:

```
KAVB3674-I Termination processing of JP1_CONS has started.
KAVB3662-I The process management is not running.
KNAN11185-I Processing to stop the IM database service will now start.
KNAN11028-I Please wait.
KNAN11187-I The IM database service stopped normally.
KNAN11186-I Processing to stop the IM database service ended normally.
KNAN11188-I The status of the IM database service will now be confirme
d.
KNAN11183-I The IM database service is stopped.
KNAN11189-I The status of the IM database service was successfully conf
irmed.
```

Example 5

JP1/IM - Manager and the intelligent integrated management database are running:

Input value:

```
jco_stop
```

Result:

```
KAVB3674-I Termination processing of JP1_CONS has started.
KAVB3675-I The stop command terminated normally
KNAN12063-I Termination processing of Trend Data Management Service ha
s started.
KNAN12067-I Trend Data Management Service stopped normally.
KNAN12065-I Processing to stop Trend Data Management Service ended norm
ally.
KNAN12064-I Termination processing of Intelligent Integrated DB Server
has started.
KNAN12068-I Intelligent Integrated DB Server stopped normally.
KNAN12066-I Termination processing of Intelligent Integrated DB Server
has started.
```

jco_stop.cluster (UNIX only)

Function

When you are operating in a cluster system, this command terminates JP1/IM - Manager on the logical host.

After stopping the JP1/IM - Manager, if the intelligent integrated management database service and the trend data management service on the logical host are running, terminate the intelligent integrated management database service and the trend data management service. If the IM database service is running, terminate the IM database service.

When you execute this command, the JP1/IM - Manager processes, the trend data management service, the intelligent integrated management database service and the IM database service are terminated. If this command is executed but the processes do not terminate, use the `jco_killall.cluster` command to forcibly terminate all processes.

To execute this command, you must have executed `jp1cc_setup_cluster` and `jp1cs_setup_cluster` after installing and setting up JP1/IM - Manager.

If you want to use the intelligent integrated management database service or the trend data management service, you must set up the intelligent integrated management database.

For the IM database service to use, you must have set up the cluster system for that IM database service. For details about setting up a cluster system, see *Chapter 8. Operation and Environment Configuration in a Cluster System (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Format

```
jco_stop.cluster [logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

`/etc/opt/jp1cons/`

Arguments

logical-host-name

When you are operating in a cluster system, this option specifies the name of the logical host where this command is to be executed. The permitted length is from 1 to 63 bytes characters. If this option is omitted, the command assumes the logical host name specified in the `JP1_HOSTNAME` environment variable. If the `JP1_HOSTNAME` environment variable is not specified, the command assumes the physical host name.

Note

The jco_stop.cluster command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
`1`	More than one argument is specified or the termination request resulted in a timeout

jcoappexecfcheck (Windows only)

Function

This command checks the contents of a definition file for executing applications.

The definition file for executing applications in a specified directory is checked for any definition errors. Analysis results of the checking are output to standard output.

The analysis results are output in the following format:

```
application-execution-definition-identifier,execution-path[,text]
```

The analysis results contain the application execution definition identifier defined in the system ("`default_browser`" indicating the default Web browser definition used in Central Console).

Format

```
jcoappexecfcheck application-execution-definition-directory-name
```

Execution permission

None

Storage directory

View-path`\bin\`

Arguments

application-execution-definition-directory-name

Specifies the directory containing the definition file for executing applications that is to be checked, expressed as an absolute path or a path relative to the current directory. This cannot be a file name.

Example

Execute the command to check the following definition file:

```
@file type="application-execution-definition", version="0300";
@define-block type="application-execution-def";
id="notepad";
path="C:\winnt\system32\notepad.exe";
@define-block-end;
@define-block type="application-execution-def";
id="dmp";
path="[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P\0521/A\PathName\Path00
]\bin\DMPSTS.exe";
@define-block-end;
```

The analysis results are output as follows:

```
"dmp","C:\NETMDMP\bin\DMPSTS.exe"
"notepad","C:\winnt\system32\notepad.exe"
```

```
"default_browser","C:\Program Files\Netscape\Communicator\Program\netscape.e
xe"
```

jcoattrfcheck

Function

This command checks the contents of definition files for extended event attributes.

The definition files for extended event attributes that are in a specified directory are checked for any definition errors. Analysis results of the checking are output to standard output. Error information, such as definition errors, is output to standard error.

The command outputs the analysis results in CSV format. Each line contains the following information for one event ID:

```
platform,event-ID,language-type,product-name,attribute-name,display-name,ty
pe
```

Note

The portion `,`*attribute-name*`,`*display-name*`,`*type* is output as many times as there are event attributes to be displayed.

When definition files for extended event attributes (extended file) are checked, the output of some of the fields is fixed. These fields are shown in the following table.

Table 1–28: Fixed values that are output when the extended files are checked

No.	Field	What is output
1	Platform	`base`
2	Event ID	`DEFAULT`
3	Language type	When `extend_attr_ja.conf` is checked: `japanese` When `extend_attr_en.conf` is checked: `english` When `extend_attr_zh.conf` is checked: `chinese`
4	Product name	`/HITACHI/DEFAULT`

JP1 event attributes displayed in the Event Details window contain this command's analysis results and the information common to the basic and extended attributes.

Format

```
jcoattrfcheck extended-event-attribute-definition-directory-name
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

extended-event-attribute-definition-directory-name

Specifies the name of the directory that contains the definition files for extended event attributes that are to be checked. Express the directory name as an absolute path or a path relative to the current directory.

Files to be checked must have the extension `.conf` and their file type will be `extended-attributes-definition`.

If you want to check definition files for extended event attributes (extended files), you must create an `extend` subdirectory in the directory specified in the argument of the `jcoattrfcheck` command and place the extended files in the `extend` directory. The files in the `extend` directory are checked as the extended files.

Note that, in checking the extended files, this command reads the standard files installed in JP1/IM - Manager and the extended file located in the directory specified in the argument of the `jcoattrfcheck` command, and checks whether the specified extended attributes are duplicated. The path of the standard files that are read when the extended file is checked is as follows:

In Windows

Console-path`\conf\console\attribute\default.conf`

In UNIX

`/etc/opt/jp1cons/conf/console/attribute/default.conf`

jcochafmode (UNIX only)

Function

This command changes the location of the event acquisition filter from Event Console Service to Event Base Service.

If you execute this command while you are using an event acquisition filter (for compatibility), the filter becomes applicable to the automated action functions and to Central Scope, as well as to JP1 event monitoring. You can then define detailed filter conditions. However, if you want to use the event acquisition filter (for compatibility) as is, there is no need to change the filter location.

Information specified in the event acquisition filter version 07-00 or earlier, or the event acquisition filter (for compatibility) is inherited as shown in the table below. Change the settings and condition group names as appropriate to your operation.

Table 1–29: Inheritance of event acquisition filter settings

Settings before execution of jcochafmode command	After execution of jcochafmode command
None	Inherited as `Existing conditions group` with no settings
Only event IDs are set	Inherited as `Existing conditions group`
Only event levels are set	Inherited as `Existing conditions group`
Only JP1/SES events are set	Inherited as `Existing conditions group_SES`
JP1/SES events and event IDs are set	The JP1/SES event and event ID# settings are inherited as `Existing conditions group_SES`. The event ID# settings are inherited as `Existing conditions group`.
Event levels and event IDs are set	Inherited as `Existing conditions group`
JP1/SES events and event levels are set	The JP1/SES event settings are inherited as `Existing conditions group_SES`. The event level settings are inherited as `Existing conditions group`.
JP1/SES events, event levels, and event IDs are set	The JP1/SES event and event ID# settings are inherited as `Existing conditions group_SES`. The event level and event ID# settings are inherited as `Existing conditions group`.

#

The event ID settings are inherited to both condition groups.

Format

```
jcochafmode [-h logical-host-name]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1cons/bin/`

Note: This command is not included in JP1/IM - Manager for Linux.

Arguments

`-h` *logical-host-name*

Specifies the logical host name for the event acquisition filter (for compatibility). If this option is omitted, the command assumes the physical host. If you do not use a cluster system, specification of this option is not needed.

Notes

- If you wish to execute this command to change the location and definitions of an event acquisition filter, you must first terminate JP1/IM - Manager at the target host whose event acquisition filter is to be changed. If this command is executed while the JP1/IM - Manager is running, an error results.
- If you execute this command more than once, the converted event acquisition filter is overwritten and the customized condition definitions are discarded. Execute this filter only once when you convert an event acquisition filter.
- Once you convert an event acquisition filter, you can no longer restore the previous event acquisition filter or event acquisition filter (for compatibility) to the filter location and definitions existing before upgrading.
- An event acquisition filter version 08-01 or later cannot be converted to an event acquisition filter (for compatibility).
- If you have newly installed JP1/IM - Manager, there is no need to execute this command.
- If you change the location of an event acquisition filter to Event Base Service by executing this command, that filter becomes applicable to the correlation event generation function thereafter.

Return values

`0`	Normal termination
`1`	Abnormal termination

Example

Convert the event acquisition filter (for compatibility) at the logical `host01` to the event acquisition filter that is run on Event Base Service:

```
jcochafmode -h host01
```

Output example 1

JP1/IM - Manager at the target host whose event acquisition filter is to be changed is not running:

```
KAVB1005-I The command (jcochafmode) has started.
KAVB0836-I The event acquisition filter was switched from interchangeabilit
y to the ordinary mode.
KAVB1002-I The command (jcochafmode) terminates normally.
```

Output example 2

JP1/IM - Manager at the target host whose event acquisition filter is to be changed is running:

```
KAVB1005-I The command (jcochafmode) has started.
KAVB0831-E JP1/IM - Manager has started.
KAVB1003-I The command (jcochafmode) terminates abnormally.
```

jcochcefmode

Function

This command changes the operating mode for the common exclusion-conditions of JP1/IM - Manager. Executing the command changes the common exclusion-conditions mode from *normal* to *extended*, and vice versa. If the mode is changed from *extended* to *normal*, common exclusion-conditions and additional common exclusion-conditions are not passed to the normal-mode common exclusion-conditions. To change the common exclusion-conditions mode to *extended*, the regular expressions of JP1/Base must be extended. For details about how to extend regular expressions of JP1/Base, see the *JP1/Base User's Guide*.

If you execute this command with the `-m` option specified, JP1/IM - Manager must not be running. If this command is executed without stopping JP1/IM - Manager, the command terminates with an error and a message is displayed.

In addition, multiple instances of this command cannot be executed concurrently.

Note that the operating mode of the common exclusion-conditions can be changed to *extended* when common exclusion-conditions have already been set.

The backup file of the extended definition file for the common exclusion-conditions is output as `common_exclude_filter_backup.conf` when either of the following applies:

- The operating mode is changed from *normal* to *extended,* and there is a problem with the regular expressions.
- The operating mode is changed from *extended* to *normal*.

The following shows the output destination of the backup file.

In Windows:

For a physical host:

Console-path`\conf\console\filter\`

For a logical host:

shared-folder`\jp1cons\conf\console\filter\`

In UNIX:

For a physical host:

`/etc/opt/jp1cons/conf/console/filter/`

For a logical host:

shared-directory`/jp1cons/conf/console/filter/`

If there are regular expressions that cannot be used in extended mode, an error is displayed, and extended-mode common exclusion-conditions are not set. Edit the output file, and then use the `-ef` option of the `jcochfilter` command to apply the changes to JP1/IM - Manager.

For details about the extended definition file for common exclusion-conditions, see *Common-exclusion-conditions extended definition file* in *Chapter 2. Definition Files*.

For details about the `jcochfilter` command, see *jcochfilter* in *Chapter 1. Commands*.

Format

```
jcochcefmode [-m {normal | extended}]
             [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-m {normal | extended}`

Specifies the operating mode of the common exclusion-conditions.

- `normal`: Specify this value to set the operating mode of the common exclusion-conditions to normal mode. The default value is `normal`.

  If the operating mode is changed back to *normal* from *extended*, the definition of normal-condition common exclusion-conditions becomes empty. The definition of the common exclusion-conditions used in extended mode is saved as a backup. In addition, all definitions of additional common exclusion-conditions are deleted. For details about backup files, see *Function*.
- `extended`: Specify this value to set the operating mode of the common exclusion-conditions to extended mode. The definition for the common exclusion-conditions used in normal mode is passed to the definition of the extended-mode common exclusion-conditions. Note that if the operating mode of the common exclusion conditions is changed to extended mode, the regular expressions in JP1/Base must be extended, which will affect your ability to use those regular expressions in JP1/Base. For details about extended regular expressions in JP1/Base, see the *JP1/Base User's Guide*.

`normal` and `extended` are not case sensitive.

`-h` *logical-host-name*

For operation in a cluster system, this option specifies the logical host name. The operating mode for the specified host is set in the common exclusion-conditions for JP1/IM - Manager. If this option is omitted, the logical host name specified for the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

If `JP1_DEFAULT` or a non-existent logical host is set for the `JP1_HOSTNAME` environment variable, an error is displayed.

Notes

- If the `-m` option is not specified, the operating mode in the common exclusion-conditions is displayed.
- If either of the following conditions, or both, applies, extended mode cannot be used:

    - An event acquisition filter (for compatibility) is used
    - Extended regular expressions are not used in JP1/Base on the manager host
- To change the operation mode of the common exclusion conditions on a logical host by using the `-h` option, a shared disk must be mounted.
- If you are using a cluster system, you must copy the common definition information from the active server to the standby server.

  For details about how to copy the information, see *7.8.2 Using commands to change settings (for Windows)* or *8.8.2 Using commands to change settings (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.
- The jcochcefmode command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
`1`	Abnormal termination
`2`	Argument error
`3`	JP1/IM - Manager is running
`4`	Prerequisite conditions for extended mode are not satisfied, or an event acquisition filter (for compatibility) is running
`5`	Prerequisite conditions for extended mode are not satisfied or regular expressions in JP1/Base are not extended
`6`	The same operating mode as the current mode is specified
`7`	No execution permission for the `jcochcefmode` command assigned (Windows only)
`8`	Backup of the extended definition file for common exclusion-conditions failed
`9`	Invalid logical host specification
`10`	Concurrent execution error
`255`	Other error

Example 1

Change the operating mode to normal mode:

Input value:

```
jcochcefmode -m normal
```

Result:

```
KAVB1005-I The command (jcochcefmode) has started.
KAVB0895-I The operation mode of the common exclusion conditions was ch
anged to basic mode.
KAVB1002-I The command (jcochcefmode) terminates normally.
```

Example 2

Change the operating mode to extended mode:

Input value:

```
jcochcefmode -m extended
```

Result:

```
KAVB1005-I The command (jcochcefmode) has started.
KAVB0896-I The operation mode of the common exclusion conditions was ch
anged to extended mode.
KAVB1002-I The command (jcochcefmode) terminates normally.
```

Example 3

Check the operating mode for the common exclusion-conditions (in this example, the name of the physical or logical host is `hostA`, and the operating mode is extended):

Input value:

```
jcochcefmode
```

Result:

```
KAVB1005-I The command (jcochcefmode) has started.
KAVB0894-I The operation mode of the common exclusion conditions will b
e displayed. (host name = host A)
operation mode = extended mode
KAVB1002-I The command (jcochcefmode) terminates normally.
```

jcochfilter

Function

This command switches the event acquisition filter that is enabled in the correlation event generation function and Event Base Service of JP1/IM - Manager to the event acquisition filter indicated by a specified filter ID. In addition, the specified common exclusion-conditions can be enabled or disabled.

The command can display a list of the event acquisition filter's filter IDs, filter names, common exclusion-conditions group IDs, and common exclusion-conditions group names.

If JP1/IM - Manager is not running on the specified host, and an event acquisition filter (for compatibility) is used, this command cannot be used.

In addition, if the mode of the common exclusion-conditions is extended mode, the following operations can be performed:

- Enabling or disabling of the extended-mode common exclusion-conditions for each condition group
- Reading of the definition file for common exclusion-conditions and batch-application of the definitions for extended-mode common exclusion-conditions
- Reading of the definition file for the common exclusion-conditions and checking of the definitions for extended-mode common exclusion-conditions
- Enabling or disabling of the defined additional common exclusion-conditions group for each conditions group

Format 1

```
jcochfilter [-i filter-ID]
            [-e [common-exclusion-conditions-group-ID
            [,common-exclusion-conditions-group-ID...]|ALL]]
            [-on common-exclusion-conditions-group-ID[,common-exclusion-cond
itions-group-ID...]]#
            [-off common-exclusion-conditions-group-ID[,common-exclusion-con
ditions-group-ID...]]#
            [-ef name-of-extended-definition-file-for-common-exclusion-condi
tions]#
            [-h logical-host-name]
```

#: Can be specified only for extended-mode common exclusion-conditions.

Format 2

```
jcochfilter -check name-of-extended-definition-file-for-common-exclusion-con
ditions
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-i` *filter-ID*

Specifies the filter ID of the event acquisition filter to be switched.

`-e [`*common-exclusion-conditions-group-ID*`,`*common-exclusion-conditions-group-ID*`...]|ALL`

Specifies the IDs of the common exclusion-conditions groups that you want to enable. The common exclusion-conditions whose group IDs are not specified will be disabled. If the common exclusion-conditions mode is extended mode, the ID of an additional common exclusion-conditions group can be specified. Separate multiple IDs with the comma. To enable all common exclusion-conditions, specify `ALL`.

You can specify the following values for *common-exclusion-conditions-group-ID*:

- Basic mode: `0` to `29`
- Extended mode: `0` to `2,499`

Note that if you specify nothing following `-e`, all common exclusion-conditions will be disabled. For the ID of an additional common exclusion-conditions group, specify a numeric value prefixed with `A`.

This option can be specified together only with the `-i` and `-h` options.

`-on` *common-exclusion-conditions-group-ID*`[,`*common-exclusion-conditions-group-ID*`...]`

Specifies the ID of the extended-mode common exclusion-conditions you want to enable or the ID of additional common exclusion-conditions. This option can be set only when the common exclusion-conditions mode is extended mode. If you specify multiple extended-mode common exclusion-conditions IDs, separate them with a comma (`,`). You can specify the following values for *common-exclusion-conditions-group-ID*:

- Basic mode: `0` to `29`
- Extended mode: `0` to `2,499`

For the ID of an additional common exclusion-conditions group, specify a numeric value prefixed with `A`.

This option cannot be specified together with the `-e`, `-ef`, or `-check` option.

`-off` *common-exclusion-conditions-group-ID*`[,`*common-exclusion-conditions-group-ID*`...]`

Specifies the ID of the extended-mode common exclusion-conditions that you want to disable or the ID of additional common exclusion-conditions. This option can be set only when the common exclusion-conditions mode is extended mode. If you specify multiple extended-mode common exclusion-conditions IDs, separate them with a comma (`,`). You can specify the following values for *common-exclusion-conditions-group-ID*:

- Basic mode: `0` to `29`
- Extended mode: `0` to `2,499`

For the ID of an additional common exclusion-conditions group, specify a numeric value prefixed with `A`.

This option cannot be specified together with the `-e`, `-ef`, or `-check` option.

`-ef` *name-of-extended-definition-file-for-common-exclusion-conditions*

Specifies the name of the definition file for common exclusion-conditions you want to apply to JP1/IM - Manager in relative or absolute path format. This option can be set only when the common exclusion-conditions mode is extended mode. By specifying this option, you can batch-apply to JP1/IM - Manager the definitions of the extended-mode common exclusion-conditions described in the extended definition file for common exclusion-conditions#.

If an additional common exclusion-conditions group is set, all definitions are deleted. This option can be specified together only with the `-h` option.

#: The definition cannot be applied if the definition includes any environment-dependent character or other character that might cause character corruption.

`-check` *name-of-extended-definition-file-for-common-exclusion-conditions*

This option checks whether the definitions of the extended-mode common exclusion-conditions specified in the extended definition file for common exclusion-conditions are correct. This also checks whether the definitions include any environment-dependent character or other character that might cause character corruption.

Specify the name of the definition file for the common exclusion-conditions you want to apply to JP1/IM - Manager in relative or absolute path format. This option cannot be specified together with other options.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. This option cannot be specified together with the `-check` option.

Notes

- If `-h` is the only option specified, the following items are listed:
  - Filter IDs and filter names of the event acquisition filters that are currently enabled
  - IDs and names of the common exclusion-conditions groups currently enabled
  - Filter IDs and filter names of the event acquisition filters that have been set
  - IDs and names of the common exclusion-conditions groups that have been set
  - When the common exclusion-conditions operating mode is extended mode, the ID of the extended-mode common exclusion-conditions and the common exclusion-conditions group name
- If JP1/IM - Manager is not running at the specified host and the event acquisition filter is used for compatibility, the `jcochfilter` command cannot be executed.
- If you execute more than one `jcochfilter` command at the same time, it might cause an error depending on the timing.
- Executing the `jcochfilter` command concurrently many times might cause timeouts or a degraded performance of managers.
- The `jcochfilter` command cannot be executed together with the `jco_spmd_status` command.

Return values

`0`	Normal termination
`1`	Argument error
`2`	Connection cannot be established with JP1/IM - Manager (Central Console) (communication error)
`3`	Operating status of JP1/IM - Manager cannot be verified
`4`	There was no response from JP1/IM - Manager within a specific amount of time
`5`	Event acquisition filter is running in the compatibility mode
`6`	Error from JP1/IM - Manager

7	Filter ID specified in the `-i` option does not exist
8	User does not have permissions to execute the `jcochfilter` command (Windows only)
9	The maximum length for an event acquisition filter was exceeded
10	The common exclusion-conditions specified in the `-e` option do not exist
11	The common exclusion-conditions group (extended mode) specified for the `-on` or `-off` option not found
12	The common exclusion-conditions group (extended mode) cannot be used (the setting is not for extended mode)
13	Application of the definition of common exclusion-conditions group (extended mode) failed
14	The definition of common exclusion-conditions group (extended mode) contains an error
255	Other error

Example 1

List the event acquisition filters on logical host `hostA`:

```
jcochfilter -h hostA
```

Example 2

Change the filter ID of the event acquisition filter on logical host `hostA` to `3`:

```
jcochfilter -i 3 -h hostA
```

Example 3

Enable common exclusion-conditions groups (ID: 0, 2) for the event acquisition filter on the logical host (`hostA`), and disable all other groups:

```
jcochfilter -e 0,2 -h hostA
```

jcochstat

Function

This command changes information about the response status for severe events.

The command accesses the event database on the host specified in `-h` and changes the response status of the JP1 events whose serial numbers are specified in `-n`.

When a response status is changed, the change is also applied to the response status displayed by other JP1/IM - Views that are logged in to the same manager. If a JP1 event whose response status is to be changed has been forwarded from another host or is set to be forwarded to another host, the response status is not changed at the source or target host.

This command can also be used to change the response status of JP1 events that are not displayed on the **Severe Events** page in the Event Console window. In such a case, you must use one of the following methods to check the change:

- If the JP1 event whose response status has been changed is displayed on the **Monitor Events** page in the Event Console window: Check the **Monitor Events** page.
- If the JP1 event whose response status has been changed is not displayed on the **Monitor Events** page in the Event Console window: Search for the event to check its status.

You can use this command while JP1/IM - Manager is running.

Format

```
jcochstat [-h manager-host-name]
          {-k severe-event-response-status-key | -d |
           -k severe-event-response-status-key -d}
           -n serial-number-1[,...,serial-number-100]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *manager-host-name*

Specifies the manager that has the event database in which the severe events are registered. You can specify host names, domain names, and IPv4 addresses. If this option is omitted, the command assumes the logical host. If this option is omitted during cluster system operation, the command assumes the name of the physical host where the command is executed. If JP1/IM - Manager is not running at the specified manager, an error results.

Specify the manager host name as a string of from 1 to 255 characters.

Note that the ability to specify the manager of another host in *manager-host-name* is supported for compatibility with version 6.

`-k` *severe-event-response-status-key*

Specifies the key value that represents the new severe event response status. The severe event response status of the severe events specified in the `-n` option is changed to the response status indicated by this key. If you use JP1/IM - View to display the status, the response status symbol changes.

A severe event response status key is case sensitive.

You must specify one or both of the `-k` and `-d` options. When both options are specified, the command changes the response status and then deletes the events from the JP1/IM - View window. The `-k` and `-d` options cannot both be omitted.

Note

The concurrent execution of a large number of `jcochstat` commands can lead to the degradation of manager performance or cause the manager to time out.

For example, we recommend against executing the `jcochstat` command from an automated action or the like because, when the `jcochstat` command processing takes time, the processing of the action could also become delayed or the execution of the action could fail. Before incorporating the execution of the `jcochstat` command into your operation, carefully examine how the resulting operation can affect `jcochstat` command execution performance and manager performance to ensure that your operational needs are not compromised.

Table 1–30: Severe event response status keys

Key value	Response status	Response status symbol displayed in JP1/IM - View
`PROCESSED`	Processed	🏁
`PROCESSING`	Being processed	▶
`HELD`	On hold	⏸
`UNPROCESSED`	Unprocessed	(No symbol)

`-d`

Deletes the severe events specified in the `-n` option on the **Severe Events** page of the Event Console window. These events are not deleted from the event database.

A deleted event can no longer be displayed on the **Severe Events** page.

You must specify either the `-k` or `-d` option, or both.

If you specify both options, change the response status first, and then delete the event on the **Severe Events** page of the Event Console window. You cannot omit both the `-k` and `-d` options.

`-n` *serial-number*

Specifies the serial number of a severe event whose response status is to be changed. This option is mandatory. The permitted value is a decimal integer in the range from 0 to 2,147,483,647.

You can specify a maximum of 100 serial numbers. Separate multiple serial numbers with the comma. Do not specify any spaces before or after a delimiter comma.

Return values

`0`	Normal termination
`1`	Argument error

2	Network failure
3	Updating of the event database failed
4	Specified key is not supported
5	A specified event cannot be updated
7	No permission to execute the command (Windows)
255	Other error

Example

Change to processed status the response status of the events that are registered in the event database on the `host01` manager and whose serial numbers are `35` and `400`, and then delete those events from the window:

```
jcochstat -h host01 -k PROCESSED -n 35,400 -d
```

jcodbsetup

Function

This is a setup command for creating an integrated monitoring database area for storing JP1 events. You must have already specified in advance in the setup information file the database's size, port number, and storage location.

In Windows, if this command is executed in an environment where the IM Configuration Management database is not set up, the following services are registered in the OS:

- When setting up a physical host: JP1/IM-Manager DB Server, JP1/IM-Manager DB Cluster Service
- When setting up a cluster configuration: JP1/IM-Manager DB Server_*logical-host-name*, JP1/IM-Manager DB Cluster Service_*logical-host-name*

In UNIX, if this command is executed in an environment where the IM Configuration Management database is not set up, an entry containing the path to the IM database is added to the `/etc/inittab` file. The entry is added to the respective physical and logical hosts on which this command was executed. Do not delete, edit, or comment out the entry in the `/etc/inittab` file that is added when this command is executed.

Format

```
jcodbsetup {-f setup-information-file-name|-s}
           [-h logical-host-name -c {online|standby}]
           [-q]
           [-v 0]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-f` *setup-information-file-name*

Specifies the setup information file that contains the requisite information, such as the IM database installation folder and the size of the database area. If neither the IM Configuration Management database nor an integrated monitoring database has been set up, you must specify this option. If the IM Configuration Management database has already been set up, specify in this option the setup information file that you specified when you set up the IM Configuration Management database. Alternatively, if the IM Configuration Management database has already been set up, you can specify the `-s` option instead. In such a case, the command uses the setup information that was specified when the IM Configuration Management database was set up.

This option cannot be specified together with the `-s` option. Additionally, the `-f` and `-s` options cannot both be omitted.

If the path contains a space, enclose the entire path in double-quotation marks ("). If you configure a cluster environment, specify the cluster setup information file name.

-s

If the IM Configuration Management database has already been set up, you can specify this option instead of the -f option. When this option is specified, the command sets up the integrated monitoring database by using the setup information that was specified when the IM Configuration Management database was set up.

If the IM Configuration Management database has not been set up but this option is specified, the command displays the KNAN11193-E message.

This option cannot be specified together with the -f option. Additionally, the -s and -f options cannot both be omitted.

-h *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. The command sets up the integrated monitoring database for the specified logical host. If you do not use a cluster system, specification of this option is not needed. Note that this logical host name cannot be JP1_DEFAULT. In addition, the logical host name is case sensitive. For the logical host name, specify a logical host name set in JP1/Base in the correct form, especially case.

-c {online|standby}

Specifies the setup type in the cluster configuration (primary node or secondary node). If you have specified the -h option, you must specify this option. If the IM Configuration Management database has already been set up on the same host, specify the value that you used when you created the IM Configuration Management database. If you are running a logical host in a non-cluster environment, specify online.

- online: Specifies that the primary node is to be set up.
- standby: Specifies that the secondary node is to be set up.

If you specify online, mount the shared disk and establish a connection to the logical host.

-q

Specifies that the command is to be executed without requesting confirmation from the user.

-v 0

Specifies that you want to recover a backup for expansion that was backed up using a table schema from JP1/IM - Manager 09-00 to 10-50. In JP1/IM - Manager 11-00, you can specify 0 as the version of the backup for expansion.

When 0 is specified, the integrated monitoring database is set up using the same table schema as JP1/IM - Manager 09-00 to 10-50.

If the -v option is omitted, the integrated monitoring database is set up using the table schema of JP1/IM - Manager 11-00 or later.

The -v option is ignored if standby is specified for the -c option.

Return values

0	Normal termination
1	Abnormal termination

Notes

- The contents of the cluster setup information files must be identical between the primary and secondary nodes. When you set up the secondary node, copy the cluster setup information file used for the primary node and then use that file. If the contents of the files specified for the primary and secondary nodes are different, cancel the setup at the secondary node, copy the cluster setup information file from the primary node, and then re-execute the command.

- If you execute the command with the `-c` option specified, do not switch servers during execution. If you switch servers during execution, cancel the setup after the command has terminated, and then re-execute the command.
- If you have canceled the command's execution by pressing **Ctrl** + **C** or **Ctrl** + **Break**, make sure that the `pdistup`, `pdfmkfs`, `pddef`, and `pdload` processes are not executing, execute the `jcodbunsetup` command, and then re-execute this command.
- If the IM Configuration Management database has already been set up and the IM database is being used, JP1/IM - Manager Service must be stopped.
- If you are using the IM Configuration Management database in Windows, the IM database (JP1/IM3-Manager DB Server) must be running and the cluster service for the IM database (JP1/IM3-Manager DB Cluster Service) must be stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command, verify that the logical host name specified in the argument matches the JP1/Base logical host name in JP1/Base, and that the logical host name can be resolved.
- If you perform unsetup of the IM database by executing the `jcodbunsetup` or `jcfdbunsetup` command, you must restart the OS before re-executing the `jcfdbsetup` command.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jcodbunsetup

Function

This command cancels setup of the integrated monitoring database that stores JP1 events.

Execute this command when you stop using the integrated monitoring database, uninstall JP1/IM - Manager, re-create the integrated monitoring database, or expand the database size.

In an environment in which an IM Configuration Management database has been set up, the IM Configuration Management database is still available even after execution of this command.

In Windows, if this command is executed in an environment where the IM Configuration Management database is not set up, the following services are deleted:

- When removing setup of a physical host: JP1/IM-Manager DB Server, JP1/IM-Manager DB Cluster Service
- When removing setup of a cluster configuration: JP1/IM-Manager DB Server_*logical-host-name*, JP1/IM-Manager DB Cluster Service_*logical-host-name*

In UNIX, if this command is executed in an environment where the IM Configuration Management database is not set up, entries in the `/etc/inittab` file registered by the `jcodbsetup` or `jcfdbsetup` command are deleted. The entries that are deleted are only those for processing related to the physical and logical hosts on which the command was executed.

Format

```
jcodbunsetup [-h logical-host-name -c {online|standby}]
             [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. The command cancels setup of the integrated monitoring database for the specified logical host. If you do not use a cluster system, specification of this option is not needed. Note that this logical host name cannot be `JP1_DEFAULT`. In addition, the logical host name is case sensitive. For the logical host name, specify a logical host name set in JP1/Base in the correct form, especially case.

`-c {online|standby}`

Specifies the type of setup being canceled in the cluster configuration (primary node or secondary node). If you have specified the `-h` option, you must specify this option.

- `online`: Specify this value if you specified `online` during setup of the integrated monitoring database.
- `standby`: Specify this value if you specified `standby` during setup of the integrated monitoring database.

If you specify `online`, mount the shared disk and establish a connection to the logical host. In addition, if you perform unsetup of the integrated monitoring database on a logical host running in a non-cluster environment, specify `online`.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

`0`	Normal termination
`1`	Abnormal termination

Notes

- If you expand the database size in an environment in which the IM Configuration Management database has been created, you must execute the command that cancels setup of IM Configuration Management database after you've executed this command.
- If you execute the command with the `-c` option specified, do not switch servers during execution. If you switch servers during execution, re-execute the command after the command has terminated.
- If you have canceled the command's execution by pressing **Ctrl** + **C** or **Ctrl** + **Break**, make sure that the `pdirst` process is not executing, and then re-execute this command.
- In Windows, the service must be in the following status:

  For a physical host:

  The cluster service for the IM database (JP1/IM3-Manager DB Cluster Service) must be stopped, and the IM database service (JP1/IM3-Manager DB Server) must be started. In addition, if the IM Configuration Management database is set up and the IM database is being used, the JP1/IM - Manager service (JP1/IM3-Manager) must be stopped.

  For a logical host:

  The cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) on the logical host must be stopped, and the IM database service (JP1/IM3-Manager DB Server_*logical-host-name*) on the logical host must be started. In addition, when the IM Configuration Management database is set up and the IM database is being used, the JP1/IM - Manager service (JP1/IM3-Manager_*logical-host-name*) must be stopped.
- In UNIX, when the IM Configuration Management database is set up, and the IM database is being used, the JP1/IM-Manager service must be stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jcoegschange

Function

This command changes correlation event generation definitions. You can execute this command while the status of the correlation event generation function is stopped, running, or standby, but not while the status is starting or stopping.

The following notes apply to execution of the `jcoegschange` command:

- When you execute the `jcoegschange` command to change correlation event generation definitions, the new definitions take effect immediately. If there are JP1 events under correlation event generation processing when the new definitions take effect, all these events will fail.
- If no conditions are defined in the correlation event generation definition file when the `jcoegschange` command is issued, the command executes processing with no correlation event generation conditions. This means that no correlation events are issued.
- If the correlation event generation function is in running status and the correlation event generation definitions to be changed by the `jcoegschange` command contain an error, the definitions are not changed and processing continues.
- If the correlation event generation function is not running, the only processing that occurs is that the correlation event generation definitions are set. Once you start the correlation event generation function, the correlation event generation definitions take effect.
- The `jcoegschange` command cannot be executed together with the `jcoegsstatus` command in which the `-d` option is specified.

Format

```
jcoegschange [-h logical-host-name]
             -f correlation-event-generation-definition-file-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

-f *correlation-event-generation-definition-file-name*

Specifies the relative or absolute path of the correlation event generation definition file.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named /*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - /*shared-directory-name*/jp1cons
  - /*shared-directory-name*/jp1cons/conf
  - /*shared-directory-name*/jp1cons/conf/evgen
  - /*shared-directory-name*/jp1cons/conf/evgen/system

  Delete /*shared-directory-name* directory and files under it. Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

0	Correlation event generation definitions were changed successfully
1	Attempt to change correlation event generation definitions failed
2	A timeout occurred during communication with the Event Generation Service (when the integrated monitoring database is not used) or with Event Base Service (when the integrated monitoring database is used)
100	Execution permission error (Windows only)
101	Argument error
102	Communication error
255	Other abnormal termination (system error)

Example

Change the correlation event generation definitions for the physical host hostP to the definitions specified in the correlation event generation definition file /tmp/teigi1.conf:

Input value:

```
jcoegschange -f /tmp/teigi1.conf
```

Result:

```
KAJV3201-I The correlation event generation definition file (/tmp/teigi
1.conf) has been read, and the definitions for the correlation event ge
neration function on (hostP) have been updated.
```

The same result is output even if no correlation event generation definitions are set for the correlation event generation function.

jcoegscheck

Function

This command checks the contents of a correlation event generation definition file.

This command looks for definition errors and redundant definitions in the correlation event generation definition file.

Format

```
jcoegscheck -f correlation-event-generation-definition-file-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-f` *correlation-event-generation-definition-file-name*

Specifies the relative or absolute path of the correlation event generation definition file.

Return values

`0`	Contents of the correlation event generation definition file were correct
`1`	Correlation event generation definition file contained invalid contents
`100`	No execution permissions (Windows only) Execution permissions are only granted to `root` (UNIX only)
`101`	Argument error
`255`	Other abnormal termination (system error)

Example

Check the contents of correlation event generation definition file `/tmp/teigi1.conf` at the physical host `hostP`:

Input value:

```
jcoegscheck -f /tmp/teigi1.conf
```

Result (when the definitions were correct):

```
KAJV3311-I The content of the correlation event generation definition f
ile (/tmp/teigi1.conf) will now be checked.
KAJV3312-I No mistakes were found in the content of the correlation eve
nt generation definition file (/tmp/teigi1.conf).
```

Result (when there were errors in the definitions):

```
KAJV3311-I The content of the correlation event generation definition f
ile (/tmp/teigi1.conf) will now be checked.
Contents of the correlation event generation definition file (/tmp/teig
i1.conf) are now checked.
KAJV3313-E There is an invalid definition in the correlation event gene
ration definition.
KAJV3314-E There is an error in the contents of the correlation event g
eneration definition file. (file name = /tmp/teigi1.conf, line = 5, inc
orrect contents = The correlation event generation condition name has n
ot been specified.)
KAJV3314-E There is an error in the contents of the correlation event g
eneration definition file. (file name = /tmp/teigi1.conf, line = 25, in
correct contents=The number of specified event conditions exceeds the m
aximum for a single correlation event generation condition.)
```

jcoegsstart

Function

This command changes the status of the correlation event generation function from standby to running. When the correlation event generation function is placed in running status, it starts processing in accordance with the correlation event generation definitions.

You can use the `jcoegsstart` command only after you have used the `jcoegsstop` command to place the correlation event generation function on standby status. The `jcoegsstart` command cannot start the correlation event generation function when it is stopped (service start and stop are controlled by process management (`jco_spmd`)).

When the status is changed successfully by the `jcoegsstart` command, a JP1 event (`00003F25`) is issued. For details about the `00003F25` JP1 event, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

If the correlation event generation function is already in running status when the `jcoegsstart` command is executed, the status remains unchanged.

Format

```
jcoegsstart [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Return values

0	Correlation event generation function restarted successfully
1	Restart of the correlation event generation function failed
2	A timeout occurred during communication with the correlation event generation function
100	No execution permissions (Windows only).

	In UNIX, execution permissions are only granted to `root`.
`101`	Argument error
`102`	Communication error
`255`	Other abnormal termination (system error)

Example

Restart the correlation event generation function at the physical host `hostP`:

Input value:

```
jcoegsstart
```

Result:

```
KAJV3291-I The correlation event generation function for hostP has rest
arted.
```

jcoegsstatus

Function

This command displays the status of the correlation event generation function and the start options. By using the options, you can also display the correlation event generation definitions that are currently in use and the date and time at which correlation event generation definitions were applied.

Format

```
jcoegsstatus [-h logical-host-name]
             [-d]
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-d`

Specifies that the following are to be displayed: the status of the correlation event generation function, start options, correlation event generation definitions that are currently in use, and the date and time at which the correlation event generation definitions were applied by the `jcoegschange` command.

The `jcoegsstatus` command with the `-d` option specified cannot be executed together with the `jcoegschange` command.

Output format

In Windows and UNIX (when the LANG environment variable is not C)

When you execute the `jcoegsstatus` command, the status of the correlation event generation function is displayed in the following format:

```
KAJV3261-I The status of the correlation event generation service for hostP
will now be displayed.
Correlation event generation function: status
```

```
Start option : start-option
```

When the -d option is specified, the status is displayed in the following format:

```
KAJV3261-I The status of the correlation event generation service for hostP
will now be displayed.
Correlation event generation function: status
Start option : start-option
KAJV3281-I The correlation event generation definition for hostP will now
be displayed.
File name : absolute-path-of-file
Reflection time : YYYY/MM/DD hh:mm:ss
VERSION=0002
# comment
[generation-condition-name]
TARGET=filtering-condition-for-the-correlation-target-range
CON=event-condition
SAME_ATTRIBUTE=duplicate-attribute-value-condition
CORRELATION_NUM=maximum-correlation-number
TIMEOUT=timeout-period
TYPE=event-correlation-type
SUCCESS_EVENT=correlation-event-information
```

In UNIX (when the LANG environment variable is C)

When you execute the jcoegsstatus command, the status of the correlation event generation function is displayed in the following format:

```
KAJV3261-I The status of the correlation event generation service for host-
name will now be displayed.
Correlation event generation function : status
Start option : start-option
```

When the -d option is specified, the status is displayed in the following format:

```
KAJV3261-I The status of the correlation event generation service for host-
name will now be displayed.
Correlation event generation function : status
Start option : start-option
KAJV3281-I The correlation event generation definition for host-name will now
be displayed.
File name : absolute-path-of-file
Reflection time : YYYY/MM/DD hh:mm:ss
VERSION=0002
# comment
[generation-condition-name]
TARGET=filtering-condition-for-the-correlation-target-range
CON=event-condition
SAME_ATTRIBUTE=duplicate-attribute-value-condition
```

```
CORRELATION_NUM=maximum-correlation-number
TIMEOUT=timeout-period
TYPE=event-correlation-type
SUCCESS_EVENT=correlation-event-information
```

The following table lists and describes the character strings that are displayed as *status*.

Table 1–31: Character strings displayed as status

Character string displayed as status	Operating status	Description
`STARTING`	Starting	The correlation event generation function is executing startup processing.
`RUNNING`	Running	The correlation event generation function is running and is ready to perform correlation event generation processing. This status occurs in the following cases: • The correlation event generation function has started. • The `jcoegsstart` command is executed while the correlation event generation function is in standby status.
`STANDBY`	Standby	The correlation event generation function is running, but correlation event generation processing has stopped. Correlation event generation processing is not performed on a JP1 event that is issued while the function is in standby status. Even when the function status changes from standby to running, the correlation event generation processing is not performed on a JP1 event that was issued while the function was in standby status. *Remarks:* A correlation event that was being generated before the function was placed in standby status results in a failure after the function is placed in standby status.
`STOPPING`	Stopping	The correlation event generation function is engaged in termination processing.
`STOP`	Stopped	The correlation event generation function has stopped.

The following table lists and describes the character strings that are displayed as *start-option*.

Table 1–32: Character strings displayed as start-option

Character string displayed as start-option	Start option	Description
`cold`	Cold start	Do not inherit the information that was under correlation event generation processing when the function went into stop status during the previous session.
`warm`	Warm start	Inherit the information that was under correlation event generation processing when the function went into stop status during the previous session.

For details about the format of a correlation event generation definition file, see *Correlation event generation definition file* in *Chapter 2. Definition Files*.

Return values

0	Status was displayed successfully
1	Status display failed
2	A timeout occurred during communication with the correlation event generation function

`100`	No permission to execute the command (Windows)
`101`	Argument error
`102`	Communication error
`255`	Other abnormal termination (system error)

Example 1

Display the status of the correlation event generation function on the physical host `hostP` (status: running; start option: `cold`):

Input value:

```
jcoegsstatus
```

Result:

```
KAJV3261-I The status of the correlation event generation service for h
ostP will now be displayed.
Correlation event generation function : RUNNING
Start option                          : cold
```

Example 2

Display the status of the correlation event generation function on the physical host `hostP` and the correlation event generation definitions (status: running; start option: `cold`):

Input value:

```
jcoegsstatus  -d
```

Result:

```
KAJV3261-I The status of the correlation event generation service for h
ostP will now be displayed.
Correlation event generation function : RUNNING
Start option                          : cold

KAJV3281-I The correlation event generation definition for hostP will n
ow be displayed.
File name          :  /tmp/teigi1.conf
Reflection time :  2005/11/05 20:35:30

VERSION=2
[CONDITION]
TARGET=B.SOURCESERVER==host1;host2;host3
CON=CID:1, B.ID==100, E.SEVERITY==Emergency;Critical;Alert;Error
SAME_ATTRIBUTE=B.SOURCESERVER
CORRELATION_NUM=20
SUCCESS_EVENT=B.ID:A00, E.SEVERITY:Emergency, B.MESSAGE:$EV1_B.MESSAGE
```

Example 3

Display the status of the correlation event generation function on the physical host `hostP` and the correlation event generation definitions (status: standby; start option: `warm`):

The following condition applies:

- When JP1/IM - Manager is newly installed
  KAJV3283-I is displayed because the correlation event generation definition file has not been set.

Input value:

```
jcoegsstatus -d
```

Result:

```
KAJV3261-I The status of the correlation event generation service for h
ostP will now be displayed.
Correlation event generation function : STANDBY
Start option                          : warm

KAJV3283-I The correlation event generation definition for hostP has no
t been defined.
```

Example 4

Display the status of the correlation event generation function on the physical host hostP and the correlation event generation definitions (status: stopped (process down); start option: cold):

Input value:

```
jcoegsstatus  -d
```

Result:

```
KAJV3261-I The status of the correlation event generation service for h
ostP will now be displayed.
Correlation event generation function : STOP
Start option                          : cold

KAJV3281-I The correlation event generation definition for hostP will n
ow be displayed.
File name            :  /tmp/teigi1.conf
Reflection time :  2005/11/05 20:35:30

VERSION=2
[CONDITION]
TARGET=B.SOURCESERVER==host1;host2;host3
CON=CID:1, B.ID==100, E.SEVERITY==Emergency;Critical;Alert;Error
SAME_ATTRIBUTE=B.SOURCESERVER
CORRELATION_NUM=20
SUCCESS_EVENT=B.ID:A00, E.SEVERITY:Emergency, B.MESSAGE:$EV1_B.MESSAGE
```

Example 5

Load an invalid correlation event generation definition file while the correlation event generation function is running:

Input value:

```
jcoegsstatus  -d
```

Result:

```
KAJV3261-I The status of the correlation event generation service for h
ostP will now be displayed.
Correlation event generation function : RUNNING
Start option                          : cold

KAJV3281-I The correlation event generation definition for hostP will n
ow be displayed.
File name             :  /tmp/teigi1.conf
Reflection time :  2005/11/05 20:35:30

KAJV3285-I  Operations will continue while ignoring an invalid correlat
ion event generation definition of hostP.

[CONDITION]
CON=CID:1, B.ID==ZZZ    ...#Message ID is invalid
SUCCESS_EVENT=B.ID:A00, E.SEVERITY:Emergency, B.MESSAGE:$EV1_B.MESSAGE
```

jcoegsstop

Function

This command changes the status of the correlation event generation function from running to standby. When the correlation event generation function is placed in standby status, it stops correlation event generation processing.

Use the `jcoegsstop` command when you want to stop correlation event generation processing without stopping the correlation event generation function. To restore the correlation event generation function to running status, either execute the `jcoegsstart` command or restart JP1/IM - Manager.

When the status is changed successfully by the `jcoegsstop` command, a JP1 event (`00003F26`) is issued. For details about the `00003F26` JP1 event, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

Format

```
jcoegsstop [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Notes

- If you execute this command during correlation event generation processing, all correlation events undergoing generation processing will result in failure.
- A JP1 event that is issued while the correlation event generation function is in standby status is not subject to correlation event generation processing.
- If the correlation event generation function is already in standby status when the `jcoegsstop` command is executed, the status remains unchanged.

Return values

`0`	Correlation event generation function was terminated successfully
`1`	Termination of the correlation event generation function failed
`2`	A timeout occurred during communication with the correlation event generation function
`100`	No execution permissions (Windows only) Execution permissions are only granted to `root` (UNIX only)
`101`	Argument error
`102`	Communication error
`255`	Other abnormal termination (system error)

Example

Terminate the correlation event generation function on the physical host `hostP`:

Input value:

```
jcoegsstop
```

Result:

```
KAJV3301-I The correlation event generation function for hostP has stop
ped.
```

jcoevtreport

Function

This command outputs to a CSV file information about the JP1 events registered in the integrated monitoring database. Only one instance of this command can be executing at the same time.

The `jcoevtreport` command can output JP1 event information to a CSV file as long as the IM database service is running, even if the integrated monitoring database is disabled or Central Console is not running.

> **Important**
>
> Because the `jcoevtreport` command acquires an event from the integrated monitoring database, operations such as searching for events from JP1/IM - View, switching response statuses, and acquiring events from JP1/IM - Manager are affected. Therefore, if the `jcoevtreport` command is executed when many events are running, other processes of JP1/IM - View or JP1/IM - Manager are delayed, and overall operation might be affected. If you want to execute the `jcoevtreport` command, do so during a time when it will not affect operation.

For details about the CSV output format, see *4.15.2 Saving event information in the integrated monitoring database (CSV report)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The command outputs error information to standard error, such as invalid definitions or a file size that exceeds the maximum value.

The following table describes the output functions.

Function	Description
Output of event report	Function that outputs to a CSV file information about the JP1 events registered in the integrated monitoring database
Output of maintenance information	Function that outputs all information about the JP1 events registered between an output start date/time and an output end date/time in the event of an integrated monitoring database failure
Output-and-save	Function that saves JP1 event information from the output of event report function before the information is deleted from the integrated monitoring database
Output-and-save status display	Function that displays the size and percentage of the JP1 events in the integrated monitoring database that have not been output and saved (percentage representing the ratio between the events that have not been output and the maximum number of records in the integrated monitoring database), as well as the deletion warning notification level

Format

Output of event report

```
jcoevtreport [-h logical-host-name]
             [-o output-file-name]
              -s output-start-date -e output-end-date
             [-user]
             [-f filter-file-name-for-output-of-event-report]
             [-k item-file-name-for-output-of-event-report]
             [-t {ON|OFF}]
             [-a {EVTATTR|DISP}]
```

Output of maintenance information

```
jcoevtreport [-h logical-host-name]
             [-o output-file-name]
              -s output-start-date -e output-end-date
              -sys
```

Output-and-save

```
jcoevtreport [-h logical-host-name]
             [-o output-file-name]
              -save
             [-t {ON|OFF}]
             [-a {EVTATTR|DISP}]
```

Output-and-save status display

```
jcoevtreport [-h logical-host-name]
              -showsv
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host that executes the command. The command acquires JP1 event information from the integrated monitoring database that is running at the specified logical host and performs output of event reports, output of maintenance information, output-and-save, or output-and-save status display. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-o` *output-file-name*

Specifies the relative or absolute path name of the CSV file to which the JP1 event information acquired from the integrated monitoring database is to be output.

If you specify a file name that begins with a hyphen (`-`), use a relative or absolute path that includes a directory (such as `./-hoge`) in order to distinguish the file name from an option. The permitted file name is a maximum of 250 bytes including the path.

Note that the following characters cannot be specified in a file name in Windows:

- Characters: `: ? " < > |`

- A character string that completely matches any of the following strings (not case sensitive): CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9

The following describes the relationship between the specified output file name and the file name that is actually created.

Event information in the integrated monitoring database is output to a CSV file named *output-file-name_serial-number*.csv. The serial number is a number from 000 to 999. A maximum of 50,000 event information items can be output to a file. If a file with the same name already exists, the command does not overwrite the file. Instead, the command creates a new file by incrementing the serial number until an unused file name is obtained. If the serial number exceeds 999, the command ends without creating a file. If this option is omitted, the command outputs a CSV file named jcoevtreport_*serial-number*.csv to the current directory.

If the current directory (.) or the root directory (/) is specified in the file name, the command handles it as shown below:

-o argument	Windows	UNIX
.	._*xxx*.csv is created in the current directory.	_*xxx*.csv is created in the current directory.
/	_*xxx*.csv is created in the root directory.	_*xxx*.csv is created in the root directory.
"" (null character)	_*xxx*.csv is created in the current directory.	Insufficient argument error

-s *output-start-date*

Specifies the start date/time of the event arrival time that is used for outputting events.

The specification format is *YYYYMMDDhhmmss*.

The specified date/time must be within the period from 1970/01/01 00:00:00 to 2099/12/31 23:59:59 (GMT). When the time zone of the host on which the command is executed is Japan, the period is (GMT + 9:00) 1970/01/01 09:00:00 to 2099/12/31 23:59:59.

-e *output-end-date*

Specifies the end date/time of the event arrival time that is used for outputting events .

The specification format is *YYYYMMDDhhmmss*.

The specified date/time must be within the same period as for the -s option.

-k *item-file-name-for-output-of-event-report*

Specifies the relative or absolute path name of the item file name for output of event report.

If you specify a file name that begins with a hyphen (-), use a relative or absolute path that includes a directory (such as ./-hoge) in order to distinguish the file name from an option.

For details about the format of the item file for event report output, see *Item file* in *Chapter 2. Definition Files*.

-f *filter-file-name-for-output-of-event-report*

Specifies the name of a filter file in relative or absolute path format.

If you specify a file name that begins with a hyphen (-), use a relative or absolute path that includes a directory (such as ./-hoge) in order to distinguish the file name from an option.

For details about the filter file formats, see *Filter file* in *Chapter 2. Definition Files*.

-t {ON|OFF}

Specifies whether the registration time, arrival time, and START_TIME and END_TIME (common information for the extended attributes) are to be output in the format *YYYYMMDDhhmmss* or in absolute time in seconds.

- ON: Specifies that the registration time, arrival time, and START_TIME and END_TIME (common information for the extended attributes) are to be output in the format *YYYYMMDDhhmmss* (i.e., they are to be converted from absolute time in seconds from January 1, 1970, to the calendar format *YYYYMMDDhhmmss*).

- `OFF`: Specifies that the time is not to be converted to the calendar format.

This option takes precedence over the item file specification.

`ON` and `OFF` are not case sensitive.

`-a {EVTATTR|DISP}`

Specifies the output format for the header. If the `-a` option is omitted, no header is output.

When `EVTATTR` is specified, the command displays attribute names (such as `B.ID` and `E.SEVERITY`); when `DISP` is specified, the command displays item names (such as event ID and severity).

`EVTATTR` and `DISP` are not case sensitive.

If `DISP` is specified in the `-a` option, the character string to be output varies according to the value set for the LANG environment variable. Note that the `LANG` environment variable that is used to display the character string in the header depends on the OS. In Windows, the language of the header character string will be the language of the OS. In UNIX, the `LANG` environment variable that is used is the variable of the prompt where the command is executed.

In addition, when program-specific extended attributes and user-defined item names are specified in the definition file for extended event attributes (extended file), you can assign one column per attribute for output to a CSV file, in the same way as for basic attributes and common extended attributes. You can also output the names of attributes and specified items to the header. For details about the CSV output format, see *4.15.2 Saving event information in the integrated monitoring database (CSV report)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Specify whether you want to enable the function for assigning a column to each program-specific extended attribute for output in the environment definition file for event report output (`evtreport.conf`). For details, see *Environment definition file for event report output (evtreport.conf)* in *Chapter 2. Definition Files*.

The following table shows the character strings for the header that is output by the `jcoevtreport` command.

Table 1–33: Header character string output by the jcoevtreport command

-a EVTATTR	-a DISP	
	LANG is Japanese	LANG is English
B.SEQNO	Serial number	Serial number
B.ID	Event ID	Event ID
B.PROCESSID	Source process ID	Source process ID
B.TIME	Registered time	Registered time
B.ARRIVEDTIME	Arrived time	Arrived time
B.REASON	Registered reason	Registered reason
B.USERID	Source user ID	Source user ID
B.GROUPID	Source group ID	Source group ID
B.USERNAME	Source user name	Source user name
B.GROUPNAME	Source group name	Source group name
B.SOURCESERVER	Registered host name	Source event server name
B.DESTSERVER	Destination event server name	Destination event server name
B.SOURCEIPADDR	Source IP address	Source IP address
B.DESTIPADDR	Destination IP address	Destination IP address
B.SOURCESEQNO	Source serial number	Source serial number
B.CODESET	Code set	Code set

-a EVTATTR	-a DISP	
	LANG is Japanese	LANG is English
B.MESSAGE	Message	Message
E.SEVERITY	Event level	Event level
E.USER_NAME	User name	User name
E.PRODUCT_NAME	Product name	Product name
E.OBJECT_TYPE	Object type	Object type
E.OBJECT_NAME	Object name	Object name
E.ROOT_OBJECT_TYPE	Root object type	Root object type
E.ROOT_OBJECT_NAME	Root object name	Root object name
E.OBJECT_ID	Object ID	Object ID
E.OCCURRENCE	Occurrence	Occurrence
E.START_TIME	Start time	Start time
E.END_TIME	End time	End time
E.RESULT_CODE	Return code	Result code
E.JP1_SOURCEHOST	Event source host name	Event source host
E.JP1_GENERATE_SOURCE_SEQNO	Relation Event serial number	Relation Event serial number
E.JP1_GENERATE_NAME	Correlation event generation condition name	Correlation event generation condition name
E.JP1_IMSUPPRESS_ID	Suppressed event ID	Suppressed event ID
E.JP1_IMSUPPRESS_NAME	Repeated event condition name	Repeated event condition name
E.JP1_TRAP_NAME	Monitoring target name	Monitoring target name
E.JP1_TRAP_ID	Monitoring ID number	Monitoring ID number
E.JP1_IMCOMEXCLUDE_ID	Common exclude conditions group ID	Common exclude conditions group ID
E.JP1_IMCOMEXCLUDE_NAME	Common exclude conditions group name	Common exclude conditions group name
E.JP1_IMCOMEXCLUDE_TARGET	Common exclude conditions group target-for-exclusion	Common exclude conditions group target-for-exclusion
E.@JP1IM_ACTTYPE	Action type	Action type
E.@JP1IM_ACTCONTROL	Action	Action
E.@JP1IM_SEVERE	Server event	Severe Event
E.@JP1IM_CORRELATE	Correlation event	Correlation event
E.@JP1IM_RESPONSE	Response-waiting event	Response-waiting event
E.@JP1IM_ORIGINAL_SEVERITY	Original severity level	Original Severity Level
E.@JP1IM_CHANGE_SEVERITY	New severity level	New Severity Level
E.@JP1IM_DEALT	Response status	Event status
E.@JP1IM_RELEASE	Severe event released	Severe Event Released

-a EVTATTR	-a DISP	
	LANG is Japanese	LANG is English
`E.@JP1IM_DISMISSED`	Severe event deleted	Severe Event Deleted
`E.@JP1IM_MEMO`	Memorandum	Memo
`E.@JP1IM_DISPLAY_MESSAGE`	Changed display message	Display Message
`E.@JP1IM_CHANGE_MESSAGE`	New display message	New Message
`E.@JP1IM_CHANGE_MESSAGE_NAME`	Display message change definition	Message change definition name
`E.`*xxxxxxx*#1	Item name#2	Item name#3
Program-specific extended attributes count	Number of program-specific extended attributes#4	Program-specific extended attributes count
Program-specific extended attributes	Program-specific extended attribute	Program-specific extended attribute

#1: The name of the attribute specified in the definition file for extended event attributes (extended file) will be output.

#2: The Japanese name of the item specified in the definition file for extended event attributes (extended file) will be output.

#3: The English name of the item specified in the definition file for extended event attributes (extended file) will be output.

#4: The total number of program-specific extended attributes that are not specified in the definition file for extended event attributes (extended file) will be output.

`-user`

Specifies that an event report on the JP1 events registered in the integrated monitoring database is to be output.

The `-user` option is optional.

If you omit all of the `-user`, `-sys`, `-save`, and `-showsv` options, the output of event report function is assumed.

`-sys`

Specifies that maintenance information on the JP1 events registered in the integrated monitoring database is to be output.

`-save`

Specifies that all JP1 events in the integrated monitoring database that have not been output and saved are to be output and saved.

`-showsv`

The following items are output.

Display item	Description
Percentage of the events that have not been output	The percentage of the JP1 events in the integrated monitoring database that have not been saved and output (percentage representing the ratio between the events that have not been output and the maximum number of records in the integrated monitoring database) is displayed.
Size of the events that have not been output	The data size of the JP1 events in the integrated monitoring database that have not been saved and output is displayed in megabytes. The displayed size is the data size in the integrated monitoring database. For CSV output, capacity equivalent to the displayed size of the events that were not output × 1.2 is required.
Deletion warning notification level setting	The value set for the deletion warning notification is displayed. If deletion warning notification is disabled, a hyphen (-) is displayed.

Return values

0	Normal termination
1	Invalid option or argument
2	Invalid filter
3	Invalid item file
4	Report output processing error
5	Execution permission error (Windows only)
6	Concurrent execution error
7	Serial number of the output file has reached the maximum value
101	Integrated monitoring database has not been set up
102	IM database service is not running
103	Error occurred in the connection with the IM database service
254	Memory shortage occurred
255	System error

Notes

Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

Example 1

Output to a report the events that arrived at the manager from 2008/06/01 12:00:00 to 2009/01/01/00:00:00:

```
jcoevtreport -s 20080601120000 -e 20090101000000 -user
```

Example 2

Set `report_`*xxx*`.csv` as the output destination and output an event report on the JP1 events dated from 2009/07/08 08:45:00 to 2009/07/14 17:15:00:

```
jcoevtreport -s 20090708084500 -e 20090714171500 -o report
```

Example 3

Set `report_`*xxx*`.csv` as the output destination and output maintenance information on the JP1 events dated from 2009/07/08 08:45:00 to 2009/07/14 17:15:00:

```
jcoevtreport -sys -s 20090708084500 -e 20090714171500 -o report
```

Example 4

Set `report_`*xxx*`.csv` as the output destination and perform output-and-save:

```
jcoevtreport -save -o report
```

Example 5

Displays the output-and-save status:

```
jcoevtreport -showsv
```

jcofuncfcheck (Windows only)

Function

This command checks for definition errors in the definition files for executing applications and the definition file for the Tool Launcher window in a specified directory, and then outputs the analysis results to standard output.

The analysis results are output in the following formats:

`Function tree definition`

tree-hierarchy `"`*displayed-character-string*`" [,"`*execution-command-path*`"]`

`Function toolbar definition`

`row =` *column*

`"`*displayed-character-string*`"[,"`*execution-command-path*`"]`

Note:

The `Function toolbar definition` heading and information are displayed only when one of the following directories is specified as the Tool Launcher window definition directory:

View-path`\conf\function\ja`

View-path`\conf\function\en`

The analysis results contain the application execution definition identifier defined in the system (`"default_browser"` indicating the default Web browser definition used in Central Console) and the Tool Launcher window identifier (`"root"` indicating the highest node of the menu tree).

Format

```
jcofuncfcheck application-execution-definition-directory-name
              Tool-Launcher-window-definition-directory-name
```

Execution permission

None

Storage directory

View-path`\bin\`

Arguments

application-execution-definition-directory-name

Specifies the directory containing the definition files for executing applications that are to be checked, expressed as an absolute path or a path relative to the current directory. This cannot be a file name.

Tool-Launcher-window-definition-directory-name

Specifies the directory containing the definition file for the Tool Launcher window that is to be checked, expressed as an absolute path or a path relative to the current directory. This cannot be a file name.

Example

Execute the command on the following definition files:

Definition file for executing applications

```
@file type="application-execution-definition", version="0300";
@define-block type="application-execution-def";
id="notepad";
path="C:\winnt\system32\notepad.exe";
@define-block-end;
@define-block type="application-execution-def";
id="dmp";
path="[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P\0521/A\PathName\Path00
]\bin\DMPSTS.exe";
@define-block-end;
```

Definition file for the Tool Launcher window

```
@file type="function-definition", version="0300";
@define-block type="function-tree-def";
id="node1";
parent_id="root";
name="Node 1";
@define-block-end;
@define-block type="function-tree-def";
id="node11";
parent_id="node1";
name="Node 11";
icon="%JCO_INSTALL_PATH%\image\1206.gif";
execute_id="default_browser";
args="http://";
@define-block-end;
@define-block type="function-tree-def";
id="node2";
parent_id="root";
name="Node 2";
icon="%JCO_INSTALL_PATH%\image\1206.gif";
execute_id="notepad";
@define-block-end;
@define-block type="function-tree-def";
id="node3";
parent_id="root";
name="Node 3";
icon="%JCO_INSTALL_PATH%\image\1206.gif";
execute_id="dmp";
@define-block-end;
```

The analysis results are output as follows:

```
Function tree definition
  "Integrated Management"
   "Node-1"
     "Node 11","C:\Program Files\Netscape\Communicator\Program\netscape.exe"
     "Node 2","C:\winnt\system32\notepad.exe"
     "Node 3","C:\NETMDMP\bin\DMPSTS.exe"
```

```
Function toolbar definition
  row=1
   "Node 11","C:\Program Files\Netscape\Communicator\Program\netscape.exe"
   "Node 2","C:\winnt\system32\notepad.exe"
```

jcogencore

Function

With the exception of the Central Scope Service (`jcsmain`), the Intelligent Integrated Management Base Service (jddmain), these commands outputs dumps in the event of a JP1/IM - Manager process failure. After executing the `jcogencore` command, you must restart JP1/IM - Manager.

The `jcogencore` command is not a command for regular use. Execute it if a hang-up occurs in a process or if you are instructed to do so in the course of investigation by support.

To detect failures, use the health check function of JP1/IM - Manager (for details about the health check function, see *9.2 JP1/IM - Manager health check function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*).

When you execute the `jcogencore` command, it displays a message asking you to choose the processes for which failure data is to be output. Select the processes that have failed. The following table shows the files that are output when the `jcogencore` command is executed.

Table 1–34: Files that are output

OS	Process name	Name of output file	
		Java thread dump	Core dump
Windows	`evflow`	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	--
	`jcamain`	--	--
	`evtcon`[#1]	*javacore-process-ID*`ID.`*XXXXXXXXXX*`.txt`	--
	`evgen`[#1, #2]	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	--
	`jcfmain`	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	--
UNIX	`evflow`	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	`core.evflow`
	`jcamain`	--	`core.jcamain`
	`evtcon`[#1]	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	`core.java`
	`evgen`[#1, #2]	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	`core.evgen`

	`jcfmain`	*javacore-process-ID*`.`*XXXXXXXXXX*`.txt`	`core.jcfmain`
			`core.`*process-ID*`.jcfallogtrap`

Legend:

XXXXXXXXXX: Unique ID assigned automatically by the OS

--: Not output

#1

`evtcon` and `evgen` are function names.

#2

This function name is used when the integrated monitoring database is not used.

The output files are stored in the following folders:

When the process name is not `jcfmain`

In Windows:

Physical host: *Console-path*`\log\`

Logical host: *shared-disk*`\jp1cons\log\`

In UNIX:

Physical host: `/var/opt/jp1cons/log/`

Logical host: *shared-disk*`/jp1cons/log/`

When the process name is `jcfmain`

In Windows:

Physical host: *Manager-path*`\log\imcf\`

Logical host: *shared-disk*`\jp1imm\log\imcf\`

In UNIX:

Physical host: `/var/opt/jp1imm/log/imcf`

Logical host: *shared-disk*`/jp1imm/log/imcf`

In addition to the thread and core dumps that are output, other failure data can be obtained by using the data collection tool.

Once you have executed this command, you must restart JP1/IM - Manager.

- In Windows:

  Physical host: After the command has executed, stop JP1/IM - Manager Service by choosing **Control Panel**, **Administrative Tools**, **Services**, and **JP1/IM-Manager Service**, and then restart JP1/IM - Manager. After JP1/IM - Manager has restarted, use the `jco_spmd_status` command to check the process statuses.

  Logical host: After the command has executed, stop the JP1/IM-Manager_*logical-host-name* service by choosing **Control Panel**, **Administrative Tools**, and **Services**, and then restart JP1/IM - Manager. If you use cluster software to monitor the JP1/IM-Manager_*logical-host-name* service, use the cluster software to either restart the service or trigger failover.

- In UNIX:

  Physical host: After the command has executed, the selected processes are terminated forcibly. Use the `jco_stop` command to terminate all processes and then restart the processes with the `jco_start` command. After the processes have restarted, use the `jco_spmd_status` command to check the process statuses.

  Logical host: After the command has executed, the selected processes are forcibly terminated. Use the `jco_stop.cluster` command to terminate all processes and then restart the processes with the `jco_start.cluster` command. If you use cluster software to monitor JP1/IM - Manager, use the cluster software to either restart the service or trigger failover.

Format

```
jcogencore [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command outputs the thread or core dump of the JP1/IM - Manager processes at the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Notes

- When you execute the `jcogencore` command in UNIX, the processes are terminated forcibly after the dump has been output. Execute this command only in the event of process hang-up. You can use health checking to detect process hang-ups.

  Take precautions when you execute the `jcogencore` command during cluster system operation.
- Before you execute this command in UNIX, first check the available disk space on your machine. If you output a core dump for five processes (`jcfmain` excluded), the total size of the core dump might be as much as 8,419 megabytes.

  In addition, if you output a core dump for `jcfmain`, the total size of the core dump might be as much as of 560 + 230 × *number-of-jcfallogtrap-processes* megabytes.
- If multiple processes have failed, execute the following commands in the order at which they are listed:

  In Windows: Event Console Service (`evtcon`), Event Base Service (`evflow`)

  In UNIX: Event Console Service (`evtcon`), Automatic Action Service (`jcamain`), Event Base Service (`evflow`)

  You can execute the command on the correlation event generation function (`evgen`) and the IM configuration management service (`jcfmain`) in any order because there are no dependencies with other processes.
- In UNIX, the `jcogencore` command might not generate core dump files if the operating system is configured to block core dump files from being generated.

  For details about the settings for core dump files, see *2.18.10 Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Return values

`0`	Normal termination
`1`	Option or argument analysis error
`2`	Process check error
`3`	Logical host error
`4`	Execution permission error (Windows only)
`5`	Pipe creation error (Windows only)
`6`	Thread dump output processing error
`10`	Other error

Example 1

Execute the command because a hang-up occurred in the Event Console Service (`evtcon`) process on the physical host in Windows:

```
jcogencore
```

Example 2

Execute the command because a hang-up occurred in the Event Console Service (`evtcon`) process on the logical host `hostA` in Windows:

```
jcogencore -h hostA
```

Example 3

Execute the command because a hang-up occurred in the Event Console Service (`evtcon`) process on the physical host in UNIX:

```
/opt/jp1cons/bin/jcogencore
```

Example output

When a hang-up occurred in the Event Console Service (`evtcon`) process on the physical host in UNIX, and core and thread dumps were output:

```
     ProcessName    PID
[1] : evflow        1234
[2] : jcamain       94320
[3] : evtcon        3333
[4] : evgen         65654
[6] : jcfmain       3316
[7] : Exit
KAVB8427-I When outputting dumps for the three processes evflow, jcamain, an
d evtcon at the same time, output the dumps in order of evtcon, jcamain, an
d evflow.
KAVB8417-I Please enter a number for the process to output the core dump fil
e [1-7]:3
KAVB8414-I The thread dump output request has been sent.
KAVB8407-I When the core dump is output, evtcon will stop. Is this OK? (y/n)
:y
KAVB8406-I The core dump file will be output.
KAVB8416-I The core dump file has been output.
```

jcohctest

Function

This command tests the health check definition file (`jcohc.conf`) that is used by the health check function of JP1/IM - Manager to determine whether the specified definitions will execute correctly. You can test the notification command on the basis of the health check definition file.

The `jcohctest` command can be executed only when JP1/IM - Manager is running.

If you have made changes to the health check definition file (`jcohc.conf`), you cannot execute the `jcohctest` command unless you have first applied the new settings in the health check definition file by means of a method such as executing the `jco_spmd_reload` command.

During testing by the `jcohctest` command, the variables specified in the health check definition file (`HCHOST`, `HCFUNC`, `HCPNAME`, `HCPID`, `HCDATE`, and `HCTIME`) are displayed as shown below.

Table 1–35: Values displayed during execution of the jcohctest command

Variable name	Value displayed during execution of the jcohctest command
`HCHOST`	Physical host name or logical host name specified in the `-h` option
`HCFUNC`	`evflow`
`HCPNAME`	`evflow`
`HCPID`	Process ID of `evflow`
`HCDATE`	Notification command execution date (*YYYY*/*MM*/*DD*)
`HCTIME`	Notification command execution time (*hh*:*mm*:*ss*)

For details about the health check definition file (`jcohc.conf`), see *Health check definition file (jcohc.conf)* in *Chapter 2. Definition Files*.

Format

```
jcohctest [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command tests the notification command that is set in the health check definition file for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Return values

`0`	Normal termination
`1`	Argument error
`2`	Logical host does not exist
`3`	Notification command execution failure
`7`	Execution permission error (Windows only)
`10`	Other error

jcoimdef

Function

This command sets up a system environment for JP1/IM - Manager or references settings.

When this command is executed, the settings are output to standard output.

For details about the setting values that are enabled by setting the `-i` option, see the description for the `-i` option.

Format

```
jcoimdef  [-r {EXE | OUTPUT | OFF}]
          [-b event-acquisition-location]
          [-s {ON | OFF}]
          [-egs {ON | OFF}]
          [-resevent {ON | OFF}]
          [-e retry-interval]
          [-t timeout-period]
          [-c retry-count:retry-interval]
          [-o retry-count:retry-interval]
          [-i]
          [-h logical-host-name]
          [-memo {ON | OFF}]
          [-chsev {ON | OFF}]
          [-db {ON | OFF}]
          [-dbntc {ON | OFF}]
          [-dbntcpos deletion-warning-notification-level]
          [-cf {ON | OFF}]
          [-cmdbtn {ON | OFF}]
          [-hostmap {ON | OFF}]
          [-bizmonmode {ON | OFF}]
          [-ignorecasehost {ON | OFF}]
          [-storm {ON | OFF}]
          [-dd {ON | OFF}]
```

The `-resevent` option is used for linking with BJEX or JP1/AS. For details about the `-resevent` option, see *11.5.1 jcoimdef* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

No arguments specified

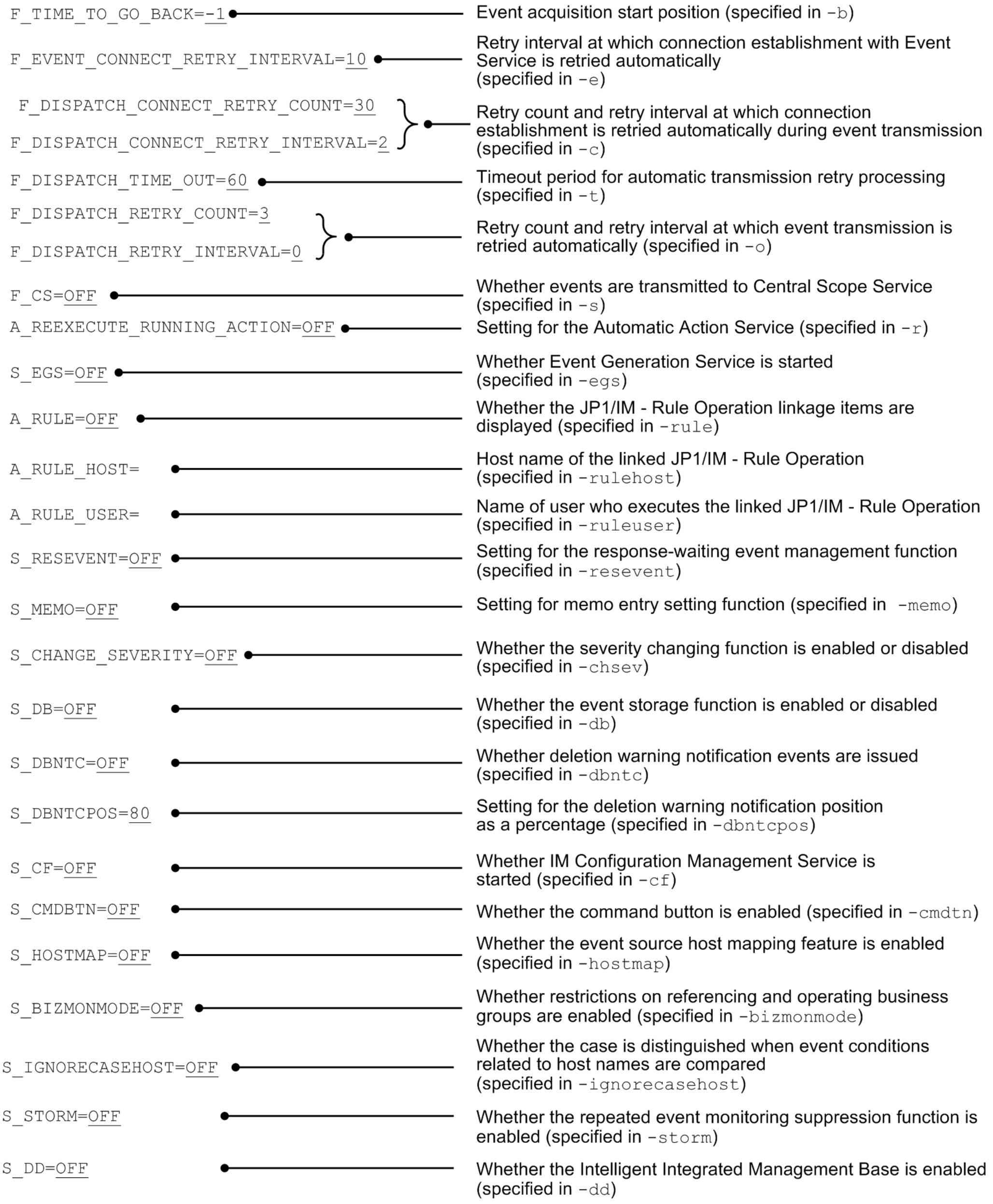
Specifies that a list of current settings is to be displayed at standard output.

The display format is as follows:

setting-item-name=setting

The figure below shows the information that is output by this command when the default values are used. You can change the settings for the items by specifying arguments.

Figure 1–1: jcoimdef command output format



```
F_TIME_TO_GO_BACK=-1
F_EVENT_CONNECT_RETRY_INTERVAL=10
F_DISPATCH_CONNECT_RETRY_COUNT=30
F_DISPATCH_CONNECT_RETRY_INTERVAL=2
F_DISPATCH_TIME_OUT=60
F_DISPATCH_RETRY_COUNT=3
F_DISPATCH_RETRY_INTERVAL=0
F_CS=OFF
A_REEXECUTE_RUNNING_ACTION=OFF
S_EGS=OFF
A_RULE=OFF
A_RULE_HOST=
A_RULE_USER=
S_RESEVENT=OFF
S_MEMO=OFF
S_CHANGE_SEVERITY=OFF
S_DB=OFF
S_DBNTC=OFF
S_DBNTCPOS=80
S_CF=OFF
S_CMDBTN=OFF
S_HOSTMAP=OFF
S_BIZMONMODE=OFF
S_IGNORECASEHOST=OFF
S_STORM=OFF
S_DD=OFF
```

Event acquisition start position (specified in `-b`)

Retry interval at which connection establishment with Event Service is retried automatically (specified in `-e`)

Retry count and retry interval at which connection establishment is retried automatically during event transmission (specified in `-c`)

Timeout period for automatic transmission retry processing (specified in `-t`)

Retry count and retry interval at which event transmission is retried automatically (specified in `-o`)

Whether events are transmitted to Central Scope Service (specified in `-s`)

Setting for the Automatic Action Service (specified in `-r`)

Whether Event Generation Service is started (specified in `-egs`)

Whether the JP1/IM - Rule Operation linkage items are displayed (specified in `-rule`)

Host name of the linked JP1/IM - Rule Operation (specified in `-rulehost`)

Name of user who executes the linked JP1/IM - Rule Operation (specified in `-ruleuser`)

Setting for the response-waiting event management function (specified in `-resevent`)

Setting for memo entry setting function (specified in `-memo`)

Whether the severity changing function is enabled or disabled (specified in `-chsev`)

Whether the event storage function is enabled or disabled (specified in `-db`)

Whether deletion warning notification events are issued (specified in `-dbntc`)

Setting for the deletion warning notification position as a percentage (specified in `-dbntcpos`)

Whether IM Configuration Management Service is started (specified in `-cf`)

Whether the command button is enabled (specified in `-cmdtn`)

Whether the event source host mapping feature is enabled (specified in `-hostmap`)

Whether restrictions on referencing and operating business groups are enabled (specified in `-bizmonmode`)

Whether the case is distinguished when event conditions related to host names are compared (specified in `-ignorecasehost`)

Whether the repeated event monitoring suppression function is enabled (specified in `-storm`)

Whether the Intelligent Integrated Management Base is enabled (specified in `-dd`)

Legend:

___ (underscore): Indicates the default.

`-r {EXE | OUTPUT | OFF}`

This option is used for setting Automatic Action Service. For the option, specify the operation of an action whose status is any of the following when Automatic Action Service starts:

- Wait

- Wait (being canceled)
- Wait (cancellation failed)
- Sending
- Sending (being canceled)
- Sending (cancellation failed)
- Queuing
- Queuing (being canceled)
- Queuing (cancellation failed)
- Running
- Running (being canceled)
- Running (cancellation failed)

When `EXE` is specified, actions whose status is any of the above are re-executed. When the status of such an action is displayed in the Action Log window (or by executing the `jcashowa` command), the displayed status name contains `-R`.

`OUTPUT`: Outputs a list of actions whose status is any of the above to the action re-execution file (`actreaction`).

When the status of such an action is displayed (by a method such as executing the `jcashowa` command or in the Action Log window), `Ended -R` is displayed as the status.

As many sets of the following information items are output as there are actions in the action re-execution file:

`###` *date*`#`Δ*time*`#`Δ*event-ID*Δ*serial-number* `###[`*linefeed*`]`

`[u=`*execution-user-name*`][e=`*environment-variable-file-name*`][d=`*execution-host-name*`]`

execution-command`[`*linefeed*`]`

#: Date and time the re-execution function was executed.

`OFF`: Performs no processing for actions whose status is any of the above and leaves the action as is.

`-b` *event-acquisition-start-position*

Specifies the position at which event acquisition is to start when JP1/IM - Manager starts. The permitted value is from -1 to 144.

If you specify `-1`, processing continues from the status existing the last time JP1/IM - Manager was terminated. The default is that `-1` is set.

For example, if `-1` is specified, JP1/IM - Manager has received events through serial number `12000`, events with serial numbers from `10001` to `12000` (2,000 events) have been stored in the event buffer, and JP1/IM - Manager is restarted, the following takes place:

- Event buffer of JP1/IM - Manager:

  The events that were in the event buffer the last time JP1/IM - Manager was terminated (events with serial numbers from `10001` to `12000`) are stored in the event buffer again.

- Automated action:

  Automated action is performed on the events starting with the event (serial number `12001`) that immediately follows the event with serial number `12000`. The automated action processing involves matching events with action definitions.

If you specify `0`, acquisition processing starts from the first event that is registered after JP1/IM - Manager starts.

- Event buffer of JP1/IM - Manager:

  The events that are registered in the event database after the start are stored in the event buffer.

- Automated action:

The events that are registered in the event database after the start are subject to automated action processing.

If you specify a value in the range from 1 to 144, the command acquires the events from the event database starting with the event that was registered at the specified number of hours before JP1/IM - Manager started.

This value is in units of hours. For example, to collect events starting from an event that was registered 1 hour before JP1/IM - Manager startup, specify `1`.

- Event buffer of JP1/IM - Manager:

  The events that have been registered in the event database at the manager since the specified number of hours before the startup are stored in the event buffer.

- Automated action:

  The events that have been registered in the event database at the manager since the specified number of hours before the startup are subject to automated action processing.

  Note that an event that has already been processed by an automated action is no longer subject to automated action processing. In other words, action matching is performed only once per event.

In all cases, the events that are transmitted to Central Scope Service are the same as for the automated actions.

`-s {ON | OFF}`

Specifies whether Central Scope Service is to be started and whether events are to be transmitted to Central Scope Service.

If you specify `ON`, Central Scope Service starts when JP1/IM - Manager starts and events are transmitted to Central Scope Service. Also, in the Event Console window, the **Central Scope** button and menu are enabled.

If you specify `OFF`, events cannot be set to be transmitted to Central Scope Service because Central Scope Service is not started when JP1/IM - Manager starts. In this case, the **Central Scope** button and menu are disabled in the Event Console window. The default is `OFF`.

To enable the `-s` setting, you must also restart the connected JP1/IM - View.

`-egs {ON | OFF}`

Specifies whether the correlation event generation function is to be enabled.

If you specify `ON`, the following occurs when JP1/IM - Manager starts:

- If the integrated monitoring database is not used, the Event Generation Service is started.
- If the integrated monitoring database is used, the correlation event generation function of Event Base Service is enabled.

If you specify `OFF`, the following occurs when JP1/IM - Manager starts:

- If the integrated monitoring database is not used, the Event Generation Service is not started.
- If the integrated monitoring database is used, the correlation event generation function of Event Base Service is disabled.

The default is `OFF`.

`-resevent {ON | OFF}`

Specifies whether to enable the response-waiting event management function.

If you specify `ON`, the response function for JP1/IM - Manager events is enabled.

If you specify `OFF`, the response function for JP1/IM - Manager events is disabled. The default is `OFF`. The value set for this command takes effect when JP1/IM - Manager has been restarted, in which case you must also restart the connected JP1/IM - View. You cannot use the `-i` option or the `jco_spmd_reload` command to enable or disable the response-waiting event management function.

`-e` *retry-interval*

Specifies the interval at which connection establishment with the event service is to be retried automatically when a connection establishment attempt fails or connection is lost while the event service is acquiring events from Event Base Service. The permitted value is from 1 to 86,400 (seconds). This is a setting for Event Base Service.

`-t` *timeout-period*

Specifies the timeout period for retry processing when event transmission from Event Base Service to Central Scope Service or Event Console Service fails and automatic transmission is retried. The permitted value is from 1 to 3,600 (seconds). When Event Base Service issues a transmission request to Central Scope Service or Event Console Service and there is no response within the time specified in this option, Event Base Service stops event transmission to that control. This is a setting for Event Base Service.

`-c` *retry-count*`:`*retry-interval*

Specifies a retry count and a retry interval at which connection establishment is to be retried automatically if an attempt to establish connection with Central Scope Service or Event Console Service, fails or if connection is lost when events are transmitted from Event Base Service to Central Scope Service or Event Console Service. The permitted retry count is from 0 to 100, and the permitted retry interval is from 0 to 3600 (seconds). This is a setting for Event Base Service.

`-o` *retry-count:retry-interval*

Specifies a retry count and a retry interval at which events are to be transmitted automatically when event transmission from Event Base Service to Central Scope Service or Event Console Service fails. The permitted retry count is from 1 to 100, and the permitted retry interval is from 0 to 3600 (seconds). This is a setting for Event Base Service.

`-i`

Specifies that the values of the specified options are to be enabled. When this option is specified, the values set in the options specified in this command are loaded into Event Base Service and the Automatic Action Service and those values take effect.

The following options can be applied immediately by using the `-i` option:

- `-e`
- `-t`
- `-c`
- `-o`
- `-memo`
- `-cmdbtn`

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. The command sets up the system environment of JP1/IM - Manager at the specified logical host or references the settings for the specified logical host. However, the local host inherits the system environment from the physical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-memo {ON | OFF}`

Specifies whether the memo entry setting function is to be used.

If the integrated monitoring database is enabled and `ON` is specified in this option, the memo entry setting function is enabled. If `OFF` is specified, the memo entry setting function is disabled. If the integrated monitoring database is disabled, specifying `ON` in this option will not enable the memo entry setting function. The default is `OFF`.

`-chsev {ON | OFF}`

Specifies whether the severity changing function is to be used.

If the integrated monitoring database is enabled and `ON` is specified in this option, the severity changing function is enabled. If `OFF` is specified, the severity changing function is disabled. If the integrated monitoring database is disabled, specifying `ON` in this option will not enable the severity changing function. The default is `OFF`.

`-db {ON | OFF}`

Specifies whether the event storage function is to be used.

- `ON`: Enable the event storage function; events can be stored in the integrated monitoring database.
- `OFF`: Disable the event storage function; events cannot be not stored in the integrated monitoring database.

If the integrated monitoring database is disabled, specifying `ON` in this option will not enable the event storage function. The default is `OFF`.

If you want to specify `ON`, you must set up the integrated monitoring database.

If you start JP1/IM - Manager when the integrated monitoring database has not been set up, or when the IM database service is not running, Event Base Services outputs a message to the integrated trace log, and terminates abnormally.

`-dbntc {ON | OFF}`

Specifies whether a deletion warning notification event is to be issued when the number of JP1 events (expressed as the percentage of the maximum number of records in the integrated monitoring database) in the integrated monitoring database on which output-and-save has not been performed exceeds the deletion warning notification level.

- `ON`: Issue a deletion warning notification event when the ratio of JP1 events in the integrated monitoring database on which output-and-save has not been performed exceeds the deletion warning notification level.
- `OFF`: Do not issue a deletion warning notification event even if the ratio of JP1 events in the integrated monitoring database on which output-and-save has not been performed exceeds the deletion warning notification level. The default is `OFF`.

If the integrated monitoring database is disabled, specifying `ON` in this option will not result in issuance of a deletion warning notification event if the ratio of JP1 events in the integrated monitoring database on which output-and-save has not been performed has exceeded the deletion warning notification level.

`-dbntcpos` *deletion-warning-notification-level*

Specifies the number of JP1 events (expressed as the percentage of the maximum number of records in the integrated monitoring database) in the integrated monitoring database on which output-and-save has not been performed that is to trigger issuance of a deletion warning notification event.

The permitted value range is from 20 to 80 (%). The default is 80.

For example, if you specify `-dbntcpos 70`, the deletion warning notification level is set to 70%.

`-cf {ON | OFF}`

Specifies whether IM Configuration Management Service is to be started.

- `ON`: Start IM Configuration Management Service when JP1/IM - Manager starts.
- `OFF`: Do not start IM Configuration Management Service when JP1/IM - Manager starts. The default is `OFF`.

If you specify `ON`, make sure that IM Configuration Management has already been set up.

If you start JP1/IM - Manager when IM Configuration Management has not been set up or the IM database service has not started, Event Base Services outputs a message to the integrated trace log, and terminates abnormally.

`-cmdbtn {ON | OFF}`

Specifies whether to enable the command button in the Execute Command window.

- `ON`: Enables the command button. When enabled, the command button is displayed in the Execute Command window. By default, `ON` is set.

- `OFF`: Disables the command button. When disabled, the command button is not displayed in the Execute Command window.

`-hostmap {ON | OFF}`

Specifies whether to enable mapping on the event source host.

- `ON`: Enables mapping on the event source host.
- `OFF`: Disables mapping on the event source host. By default, `OFF` is set.

If the integrated monitoring database is disabled, mapping on the event source host will be disabled even when `ON` is specified.

`-bizmonmode {ON | OFF}`

Specifies whether to enable restrictions on referencing and operations by business groups.

- `ON`: Enables restrictions on referencing and operations by business groups.
- `OFF`: Disables restrictions on referencing and operations by business groups. By default, `OFF` is set.

If the integrated monitoring database, the IM Configuration Management service, or mapping on the event source host is disabled, restrictions on referencing and operations by business groups will be disabled even when `ON` is specified.

`-ignorecasehost {ON | OFF}`

Specifies whether to distinguish letter case when event conditions related to a host name are compared.

- `ON`: Letter case is ignored. However, if regular expressions are used in the comparison keyword, uppercase and lowercase are distinguished.
- `OFF`: Letter case is distinguished. By default, `OFF` is set.

The following table describes the correspondence between functions and attributes for which the case of a host name is ignored when this option is enabled.

Table 1–36: Correspondence between functions and event conditions

Function	Attribute (event condition)
Filtering using the severe event(s) filter	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Event search	When search object is the integrated monitoring database Event-issuing server name (registered host name) (`B.SOURCESERVER`) Target event server name (`B.DESTSERVER`) Event source host name (`E.JP1_SOURCEHOST`) When the search object is the event database Not supported
Filtering using the event acquisition filter (extended-mode common exclusion-conditions)	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Filtering using the view filter	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Filtering using the user filter	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Automated action	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Repeated event monitoring suppression	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`)

Function	Attribute (event condition)
	• Event source host name (`E.JP1_SOURCEHOST`)
Consolidated display of repeated events	Event conditions cannot be specified, but the `-ignorecasehost` option settings is applied.
Generating a correlation event	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Changing the severity	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Changing the display format of the message	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Outputting an event report	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`) • Event source host name (`E.JP1_SOURCEHOST`)
Event source host mapping	• Event-issuing server name (registered host name) (`B.SOURCESERVER`) • Target event server name (`B.DESTSERVER`) • Event source host name (`E.JP1_SOURCEHOST`)

`-storm {ON | OFF}`

Specifies whether to enable the repeated event monitoring suppression function.

- `ON`: Enables the repeated event monitoring suppression function.
- `OFF`: Disables the repeated event monitoring suppression function. The default is `OFF`.

If you specify `ON` when the integrated monitoring database is disabled, the repeated event monitoring function is disabled.

`-dd {ON | OFF}`

Specifies whether to start the Intelligent Integrated Management Base.

- `ON`: Starts the Intelligent Integrated Management Base when JP1/IM - Manager starts.
- `OFF`: Does not start the Intelligent Integrated Management Base when JP1/IM - Manager starts. The default is `OFF`.

If you specify `ON`, you must set up the integrated monitoring database in advance. You also must enable the event-source-host mapping.

If JP1/IM - Manager is started when the integrated monitoring database is not set up, the event-source-host mapping is disabled, or the IM database service is not running, the Intelligent Integrated Management Base terminates abnormally and outputs messages to the integrated trace log.

Return values

`0`	Normal termination
`1`	Abnormal termination
`7`	Execution permission error (Windows only)
`111`	Failed to connect to the Event Base Service (in UNIX)
`-401`	Failed to connect to the Event Base Service (in Windows)

When definition enabled

Option	Trigger event		
	Restarting of JP1/IM - Manage	Execution of the `jco_spmd_reload` command	`-i` option specified
`-r`	Y	--	--
`-b`	Y	--	--
`-s`	Y#	--	--
`-egs`	Y	--	--
`-resevent`	Y#	--	--
`-e`	Y	Y	Y
`-t`	Y	Y	Y
`-c`	Y	Y	Y
`-o`	Y	Y	Y
`-memo`	Y#	Y#	Y#
`-chsev`	Y#	--	--
`-db`	Y#	--	--
`-dbntc`	Y	Y	--
`-dbntcpos`	Y	Y	--
`-cf`	Y	--	--
`-cmdbtn`	Y	--	Y#
`-hostmap`	Y#	--	--
`-bizmonmode`	Y#	--	--
`-ignorecasehost`	Y#	--	--
`-storm`	Y#	--	--
`-dd`	Y	--	--

Legend:

Y: Enabled

--: Not applicable

#

The JP1/IM - View instance being connected must be restarted.

jcomonitorfcheck

Function

This command checks the definition file for opening monitor windows.

When this command is executed, it checks a specified definition file for opening monitor windows for any definition errors and then outputs the analysis results to standard output. Error information, such as definition errors, is output to standard error.

An analysis result is output for each event ID in the following format:

product-name, *event-ID*

start-version, *end-version*

[*subkey-name*, *attribute-name-used-as-key*

[*attribute-value-used-as-key*, *interface-name*]]

[*interface-name*, *application-execution-definition-identifier*,

command-argument, *replacement-event-attribute*]

If there is only one version specification, such as `0600`, the same value is output for both the start version and the end version. Similarly, if `ALL` is specified, `ALL` is displayed for both the start version and the end version.

If `SUBKEY` is set in the `DEF_KEY` key definition, the contents of the subkey are displayed. `SUBKEY` is duplicated if it is also used in another `DEF_KEY` key definition.

This command does not check whether the application execution definition identifier is defined in the definition file for executing applications.

Format

```
jcomonitorfcheck monitor-window-opening-definition-directory-name
```

Execution permission

In Windows: Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

In UNIX: None

Storage directory

In Windows:

Console-path`\bin\`

In UNIX:

`/opt/jp1cons/bin/`

Arguments

monitor-window-opening-definition-directory-name

Specifies the name of the monitor window opening definition directory, expressed as an absolute path or a path relative to the current directory.

Example

Execute the command for the following definition file:

```
DESC_VERSION=0300
# Monitor window transition definition file for AJS-View
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004102 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004103 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004104 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004105 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004106 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004107 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004108 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004109 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004120 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004121 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004122 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004123 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004124 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=00004125 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=000041A7 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=000041A8 INTERFACE=AJS2_MONI
TOR
DEF_KEY PRODUCT_NAME=/HITACHI/JP1/AJS2 EVENT_ID=000041A9 INTERFACE=AJS2_MONI
TOR

DEF_MTR_CALL NAME=AJS2_MONITOR EXEC_ID=jco_JP1_AJS2 PATH="-j %IM_EVC_PARAMET
ER_1%::%IM_EVC_PARAMETER_2%/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monito
r -l %IM_EVC_PARAMETER_4%" PARAM=B.SOURCESERVER,E.A0,E.A1,E.A3
```

The analysis results are as follows:

```
/HITACHI/JP1/AJS2, 41a9
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
```

```
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4109
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 41a8
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4108
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 41a7
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4107
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4106
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4125
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4105
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4124
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4104
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4123
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4103
```

```
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4122
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4102
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4121
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
/HITACHI/JP1/AJS2, 4120
 ALL, ALL
   AJS2_MONITOR, jco_JP1_AJS2, -j %IM_EVC_PARAMETER_1%::%IM_EVC_PARAMETER_2%
/%IM_EVC_PARAMETER_3% -t %JCO_JP1TOKEN% -v monitor -l %IM_EVC_PARAMETER_4%,
B.SOURCESERVER, E.A0, E.A1, E.A3
```

jcothreaddmp (Windows only)

Function

This command outputs a thread dump in the event of a JP1/IM - View failure.

A thread dump output by the `jcothreaddmp` command is stored in the following folder:

View-path`\log\`

You can use the data collection tool to collect other failure data in addition to the output thread dump.

Format

```
jcothreaddmp process-ID
```

Execution permission

None

Storage directory

View-path`\bin\`

Arguments

process-ID

Specifies the process ID of the `java.exe` process of the disabled JP1/IM - View. You can specify only one process ID. It is not permissible to omit the process ID or to specify multiple process IDs.

If you are running multiple instances of JP1/IM - View, you must determine the process ID of the JP1/IM - View that can no longer be controlled by the Windows Task Manager.

In Windows Task Manager, JP1/IM - View is displayed as `java.exe`. If another java program is running at the same time, that program is also displayed as `java.exe`, making it difficult to distinguish between the programs. For details about how to identify the process ID of JP1/IM - View, see *12.4.1(1)(b) Outputting a thread dump for JP1/IM* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Notes

- If the `jcothreaddmp` command is executed on a JP1/IM - View that is running normally, operation of JP1/IM - View may become unstable. In such a case, restart JP1/IM - View.

Return values

`0`	Normal termination
`1`	Option analysis error
`2`	Process checking error
`3`	Thread dump output request transmission error
`10`	Other error

jcovcfsetup (Windows only)

Function

This command registers into or deletes from the Windows **Start** menu the menu item for starting IM Configuration Management - View. Note that when IM Configuration Management - View is installed, it is not registered into the Windows **Start** menu.

This command works only when executed in the command prompt invoked from **Run as Administrator**.

Format

```
jcovcfsetup [-i | -u]
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

View-path`\bin\`

Arguments

If no options are specified, the command executes in the same manner as when the `-i` option is specified.

`-i`

Specifies that the menu for starting IM Configuration Management - View is to be registered into the Windows **Start** menu.

`-u`

Specifies that the menu for starting IM Configuration Management - View is to be removed from the Windows **Start** menu.

Note that if you have manually changed the menu name or its storage location, the command cannot remove the menu. In such a case, you must remove the menu manually.

Notes

The maximum length of the command arguments (in bytes) depends on the OS. Specify the command arguments within the limitation of the applicable OS.

Return values

`0`	Normal termination
`1`	Abnormal termination

Example 1

Add **Configuration Management** to the menu of JP1/IM - View:

```
jcovcfsetup or jcovcfsetup -i
```

Example 2

Remove **Configuration Management** from the menu of JP1/IM - View:

```
jcovcfsetup -u
```

jcoview (Windows only)

Function

This command opens a JP1/IM - View window.

The window to be opened depends on the option specifications, as shown below:

- Starting the Login window for JP1/IM - View
  When any option other than `-p` or `-e` is specified or no option is specified, the Login window opens.

  `-c` option is specified: The **Central Console** check box is selected in the Login window.

  `-s` option is specified: The **Central Scope** check box is selected in the Login window.

  `-h` option is specified: A value is entered in **Host to connect** in the Login window.

  `-u` option is specified: A value is entered in **User name** in the Login window.
- Opening the Event Console window and the Monitoring Tree window of JP1/IM - View
  When the `-h`, `-u`, or `-p` option is specified, the Event Console window and the Monitoring Tree window open. To open the Event Console window and the Monitoring Tree window, you must specify the `-h`, `-u`, or `-p` option.

  `-c` option is specified: The Event Console window opens.

  `-s` option is specified: The Monitoring Tree window opens.

  Neither the `-c` nor the `-s` option is specified: The Event Console window opens.
- Opening the Monitoring Tree (Editing) window of JP1/IM - View
  When the `-e` option is specified, the Monitoring Tree (Editing) window opens.

Format

```
jcoview [[[-c] [-s]]
         [-h connection-target-host-name] [-u user-name] [-p password]
         | -e]
```

Execution permission

None

Storage directory

View-path`\bin\`

Arguments

`-c`

Specifies that the Event Console window is to open.

If the password (`-p` option) is omitted, the Login window opens with the **Central Console** check box selected. This option cannot be specified together with the `-e` option.

This option is optional.

If the `-h`, `-u`, and `-p` options are specified and none of the `-c`, `-s`, and `-e` options is specified, the command assumes that the `-c` option is specified.

`-s`

Specifies that the Monitoring Tree window is to open.

If the password (`-p` option) is omitted, the Login window opens with the **Central Scope** check box selected. This option cannot be specified together with the `-e` option.

This option is optional.

`-h` *connection-target-host-name*

Specifies the name of the connection-target host. For the host name, from 1 to 255 bytes of characters are permitted. You can specify only a host where JP1/IM - Manager is running.

For the connection-target host name, you can specify the following:

- Host name defined on the host where the command is used
- Host name whose address can be resolved on the host where the command is used
- IP address

  Only addresses in IPv4 address format can be specified. Addresses in IPv6 address format cannot be specified.

This option is optional, but if you specify the `-p` option, you must also specify this option.

`-u` *user-name*

Specifies the name of a JP1 user that has been registered in the authentication server. For the JP1 user name, from 1 to 31 alphanumeric characters are permitted (for alphabetic characters, only lowercase letters are permitted).

This option is optional, but if you specify the `-p` option, you must also specify this option.

`-p` *password*

Specifies the specified user's password. For the password, from 6 to 32 alphanumeric characters are permitted. Alphabetic characters are case sensitive.

If you specify this option, you must also specify the `-h` and `-u` options.

This option is optional.

`-e`

Specifies that the Monitoring Tree (Editing) window is to open.

When you specify this option, you must not specify any other options.

This option is optional.

Important

- If you attempt to start JP1/IM - View by executing the jcoview command with an incorrect argument specified, the login window appears after either of the following messages is output:

  - KAVB0104-E Failed to authenticate the user.

  - KAVB1210-E A communication error occurred while establishing a connection.

  Cannot convert the host name into an IP address. Confirm the host name.

  Host name: <host-name>, Port number: <port-number>

  Details: <detail-information>

  In the login window displayed in this status, you may be unable to select the input fields even with the mouse to enter information in them. If this problem occurs, click the taskbar button for a program other than JP1/IM - View, and then click the login window.
- If the program jcoview.exe is executed from a command prompt where the code page is set to a value other than 932, the characters displayed on the screen might be garbled.
- If the program jcoview.exe is executed from a command prompt where the code page is set to a value other than 936, the characters displayed on the screen might be garbled.

Return values

0	Normal termination
1	Argument error
2	Insufficient memory
3	Resource acquisition failed
4	Error message creation failed
255	System error

Example 1

Start JP1/IM - View and open the Login window:

```
jcoview
```

Example 2

Start JP1/IM - View and display the Login window with `host` set in **Host to connect** and `jp1admin` set in **User name**:

```
jcoview -h host -u jp1admin
```

Example 3

Start JP1/IM - View, log in by specifying `jp1admin` as the user name, `jp1admin` as the password, and `host` as the connection-target host, and then open the Event Console window:

```
jcoview -h host -u jp1admin -p jp1admin
```

Example 4

Start JP1/IM - View, log in by specifying `jp1admin` as the user name, `jp1admin` as the password, and `host` as the connection-target host, and then open the Monitoring Tree window:

```
jcoview -s -h host -u jp1admin -p jp1admin
```

Example 5

Start JP1/IM - View, log in by specifying `jp1admin` as the user name, `jp1admin` as the password, and `host` as the connection-target host, and then open the Event Console window and the Monitoring Tree window:

```
jcoview -c -s -h host -u jp1admin -p jp1admin
```

Example 6

Start JP1/IM - View and open the Monitoring Tree (Editing) window:

```
jcoview -e
```

Example 7

You can create a command shortcut, such as for Examples 2 and 3, for each host and each user.

jcoview_log.bat (Windows only)

Function

This command is a tool for collecting data in the event of a JP1/IM - View failure. The data collected by this tool includes JP1/IM - View maintenance data, OS system information, and integrated trace logs. If JP1/IM - Manager and JP1/Base are installed on the same machine, data from JP1/IM - Manager and JP1/Base is also collected.

This tool constitutes a batch file, which cannot be customized by the user.

When you execute this tool, the target folders or files used for data collection are classified into primary and secondary data categories and the collected data is stored directly under a specified data storage folder.

The primary data, which consists of a minimum amount of logs and settings files, is collected for purposes such as identifying failures and investigating minor errors. The secondary data consists of the Windows event log, and provides the detailed information needed to investigate failures in depth.

If you execute `jcoview_log.bat` during a thread dump of JP1/IM - View, the tool displays the `KAVB8946-I` message asking whether the thread dump is to be deleted. If you enter `y`, the tool deletes the thread dump.

If necessary, compress the collected data by using a program such as a compression tool.

For details about the data that can be collected by this tool, see *12.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

The following tables show the organization of the folders directly under the data storage folder and the details of the data that is stored.

Table 1–37: Organization of the internal folders for the primary data

Folder name	Stored data
data-storage-folder`\jp1_default\imm_1st\coview`	JP1/IM - View patch information
data-storage-folder`\jp1_default\imm_1st\coview\conf`	JP1/IM - View settings and definition files
data-storage-folder`\jp1_default\imm_1st\coview\default`	Common definition information for JP1/IM - View
data-storage-folder`\jp1_default\imm_1st\coview\log`	Log files for JP1/IM - View
data-storage-folder`\jp1_default\imm_1st\oslog`	OS log information
data-storage-folder`\jp1_default\imm_1st\spool`	Integrated trace logs (32-bit)
data-storage-folder`\jp1_default\imm_1st\spoolx64`	Integrated trace logs (64-bit)

Table 1–38: Organization of the internal folders for the secondary data

Folder name	Stored data
data-storage-folder`\jp1_default\imm_2nd\oslog`	Windows event log

Format

```
jcoview_log.bat -f data-storage-folder
                [-t]
                [-q]
```

Execution permission

Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

Storage directory

View-path`\tools\`

Arguments

`-f` *data-storage-folder*

Specifies the name of the folder to which the collected data is to be output, expressed as a full path or a path relative to the location where the command is executed. If the path contains a space, enclose the entire path in double-quotation marks (`"`). This option is mandatory.

If a nonexistent folder is specified, a new folder with that name is created. If an existing folder is specified, the contents of that folder are deleted and then the specified folder is created.

`-t`

Specifies that the `hosts` and `services` files are not to be collected.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Notes

- If you wish to collect JP1/IM - View data at the same host as for JP1/IM - Manager, use the `jim_log.bat` command.
- Do not execute this tool more than once. If it is executed multiple times, collected data may be overwritten or data collection may fail.
- If a file to be collected cannot be found, the tool may display a message such as `The file was not found`; however, no action is necessary.

Return values

0	Normal termination
8	Abnormal termination

Example

Collect data in the `F:\tmp\bat` folder:

```
jcoview_log.bat -f F:\tmp\bat
```

The output results are as follows:

```
KAVB8925-I The directory does not exist. ("F:\tmp\bat")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("F:\tmp\bat\jp1_default\imm_1st")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("F:\tmp\bat\jp1_default\imm_2nd")
           The directory will be created.
Press any key to continue...
KAVB8926-I Data acquisition processing will start.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfI
nfo.exe" command will start.
KAVB8921-I The information for JP1/IM - View will be acquired.
KAVB8922-I The information for JP1/IM - View has been acquired.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8929-I The system information will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInf
o.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInfo.exe" execution
is ended. (ERRORLEVEL=0)
KAVB8922-I The system information has been acquired.
KAVB8929-I "Watson log and crash dump" will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnI
nfo.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8922-I "Watson log and crash dump" has been acquired.
KAVB8921-I Windows Eventlog(Application) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(Application) has been acquired.
KAVB8921-I Windows Eventlog(System) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(System) has been acquired.
KAVB8921-I The setup.ini of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ini of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ini of JP1/Base will be acquired.
KAVB8922-I The setup.ini of JP1/Base has been acquired.
KAVB8921-I The setup.ilg of JP1/Base will be acquired.
KAVB8922-I The setup.ilg of JP1/Base has been acquired.
KAVB8921-I The setup.ini of JP1/IM - View will be acquired.
KAVB8922-I The setup.ini of JP1/IM - View has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - View will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - View has been acquired.
KAVB8921-I The integrated trace log will be acquired.
KAVB8922-I The integrated trace log has been acquired.
KAVB8921-I The integrated installer log will be acquired.
KAVB8922-I The integrated installer log has been acquired.
KAVB8921-I The installer log file will be acquired.
```

```
KAVB8922-I The installer log has been acquired.
KAVB8921-I The hosts will be acquired.
KAVB8922-I The hosts has been acquired.
KAVB8921-I The services will be acquired.
KAVB8922-I The services has been acquired.
KAVB8921-I The registry information will be acquired.
KAVB8922-I The registry information has been acquired.
KAVB8921-I The netstat information will be acquired.
KAVB8922-I The netstat information has been acquired.
KAVB8921-I The ipconfig information will be acquired.
KAVB8922-I The ipconfig information has been acquired.
KAVB8921-I The net start information will be acquired.
KAVB8922-I The net start information has been acquired.
KAVB8921-I The set information will be acquired.
KAVB8922-I The set information has been acquired.
KAVB8918-I The data was successfully acquired.
```

jcschstat

Function

This command changes the status of monitoring nodes (monitoring objects or monitoring groups). It also clears the logs of status change events at the monitoring nodes. It cannot change the monitoring status of monitoring nodes.

You can include this command in batch processing in order to automatically initialize the status of monitoring nodes as the last processing step of error recovery, or you can use this command to automatically initialize the status of monitoring nodes after eliminating the cause of an error by linking with the help desk system.

You can use this command when the Central Scope functions are enabled.

If you execute this command while JP1/IM - Manager (Central Scope) is already processing 32 or more command requests, communication is lost at the server end, which causes this command to fail.

Format

```
jcschstat [-h logical-host-name]
          -n monitoring-node-ID-1, monitoring-node-ID-2, monitoring-node-ID
-3...
          [-s status-value]
          [-i]
          [-t timeout-period]
          [-d]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-n` *monitoring-node-ID-1*`,` *monitoring-node-ID-2*`,` *monitoring-node-ID-3*`...`

Specifies the IDs of the monitoring nodes (monitoring object IDs or monitoring group IDs) whose status is to be changed, expressed in hexadecimal notation.

You can specify a maximum of 10 monitoring node IDs. When you specify multiple IDs, separate them with the comma (`,`). The monitoring nodes are processed in the order in which they are specified.

`-s` *status-value*

Specifies the new status for the specified monitoring nodes. The status value is case sensitive. For monitoring objects, you can specify `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Normal`, `Debug`, or `Initial`. For monitoring groups, you can specify only `Initial`.

When the status of a specified monitoring node changes, the status is propagated to the higher nodes and the lower nodes are initialized.

If this option is omitted, `Initial` is assumed.

`-i`

Specifies that a confirmation message is to be displayed when the status of a monitoring node is to be changed.

`-t` *timeout-period*

Specifies a timeout period for communication with the server. The permitted value is from 1 to 32,767 (seconds). The default is 1,800 seconds (30 minutes).

`-d`

Specifies that command processing is to be canceled and the command is to be terminated with an error if a monitoring node specified in the `-n` option does not exist or if a monitoring node status change fails.

If this option is omitted, the command skips processing on any monitoring node that does not exist or on which status change processing fails, and then processes the next monitoring node.

Return values

`0`	Normal termination
`1`	Logical host name was not found
`2`	Argument error
`4`	No permission to execute the command
`12`	Insufficient memory
`32`	Data access error
`33`	Specified monitoring tree ID or monitoring node ID was not found in the database
`37`	No response from the server (connection establishment request failed)
`38`	Communication with the server failed (the server was terminated during communication or the server's connection count exceeded the maximum value)
`39`	A timeout occurred (after a request was sent to the server, the timeout period was exceeded before a response was received)
`40`	An invalid response was sent from the server
`42`	Another command or request is being processed
`43`	A monitoring node for which not monitor is set is specified in `-n`
`44`	A monitoring group is specified in `-n`
99	Other error

Example

Change the status of monitoring node ID `8` to `Error`:

```
jcschstat -n 8 -s Error
```

Example output

```
jcschstat -n 5 -s Normal
KAVB7630-I The status of the monitoring node (5) has been set to Normal.
```

jcsdbexport

Function

This command acquires monitoring object database storage information and outputs it locally to a file as a configuration file for monitoring tree. The information that is output to the file includes monitoring tree configuration information, common event monitoring conditions, and Visual Monitoring window configuration information.

You can use this command to store multiple generations of storage information in the monitoring object database. To copy the storage information in the monitoring object database to another server, execute this command and then use the `jcsdbimport` command to copy the storage information to the monitoring object database of the other server.

You can use this command when the Central Scope functions are enabled.

If you execute this command while updating data for Central Scope Service, the command terminates with an error. For example, if you execute this command while updating the server's tree from the Monitoring Tree (Editing) window or while changing the status of a monitoring node with the `jcschstat` command, the command terminates with an error.

A configuration file for monitoring tree that was output by JP1/IM - Manager version 08-10 or later cannot be imported by JP1/IM - Manager version 08-01 or earlier.

Format

```
jcsdbexport [-h logical-host-name]
            -o file-name
            [-t timeout-period]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-o` *file-name*

Specifies the full path of the file to which tree configuration information is to be output. The file name must end with `.dat`. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-t` *timeout-period*

Specifies the timeout period for communication with the server. The permitted value is from 10 to 32,767 (seconds). The default is 1,800 seconds (30 minutes).

Return values

`0`	Normal termination
`1`	Logical host name was not found
`2`	Argument error
`3`	Specified file is invalid
`4`	No permission to execute the command
`6`	No permission to access the specified file
`12`	Insufficient memory
`13`	Insufficient disk capacity
`31`	Database initialization failed at the server
`32`	Database access failed at the server
`33`	Specified monitoring tree ID or monitoring node ID was not found in the database
`37`	No response from the server (connection establishment request failed)
`38`	Communication with the server failed (the server was terminated during communication or the server's connection count exceeded the maximum value)
`39`	A timeout occurred (after a request was sent to the server, the timeout period was exceeded before a response was received)
`40`	An invalid response was sent from the server
`42`	Another command or request is being processed
`99`	Other error

Example

Output monitoring object database storage information to `c:\temp\output.dat`:

```
jcsdbexport -o c:\temp\output.dat
```

Example output

```
KAVB7670-I Exporting of the monitoring tree definition to the file c:\temp\o
utput.dat was successful.
```

jcsdbimport

Function

This command applies monitoring object database storage information that was output by the `jcsdbexport` command (monitoring tree configuration information, common event monitoring conditions, and Visual Monitoring window configuration information) to the monitoring object database of JP1/IM - Manager.

Use this command together with the `jcsdbexport` command to migrate JP1/IM - Manager monitoring object database storage information to another server.

You can use this command when the Central Scope functions are enabled.

If you execute this command while updating data for Central Scope Service, the command terminates with an error. For example, if you execute this command while updating the server's tree from the Monitoring Tree (Editing) window or while changing the status of a monitoring node with the `jcschstat` command, the command terminates with an error.

Format

```
jcsdbimport [-h logical-host-name]
            -o file-name
            [-t timeout-period]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-o` *file-name*

Specifies the full path of a file that was output by the `jcsdbexport` command and that is to be applied to the monitoring object database of JP1/IM - Manager. The file name must end with `.dat`. If the path contains a space, enclose the entire path in double-quotation marks (`"`).

`-t` *timeout-period*

Specifies the timeout period for communication with the server. The permitted value is from 10 to 32,767 (seconds). The default is 1,800 seconds (30 minutes).

Notes

Importing information with the `jcsdbimport` command initializes the status of the monitoring tree.

Return values

`0`	Normal termination
`1`	Logical host name was not found
`2`	Argument error
`3`	Specified file is invalid
`4`	No permission to execute the command
`6`	No permission to access the specified file
`12`	Insufficient memory
`31`	Database initialization failed at the server
`32`	Database access failed at the server
`34`	Format error in the configuration file for monitoring tree
`37`	No response from the server (connection establishment request failed)
`38`	Communication with the server failed (the server was terminated during communication or the server's connection count exceeded the maximum value)
`39`	A timeout occurred (after a request was sent to the server, the timeout period was exceeded before a response was received)
`40`	Invalid response was sent from the server
`41`	Specified input file was not found
`42`	Another command or request is being processed
`48`	The file is not compatible with the file version specified by the server
`99`	Other error

Example

Apply the file `input.dat` output by the `jcsdbexport` command to the monitoring object database of JP1/IM - Manager:

```
jcsdbimport -o input.dat
```

Example output

```
KAVB7660-I Importing of the monitoring tree definition from the file input.d
at was successful.
```

jcsdbsetup

Function

This command creates a new ISAM file for storing the monitoring object database. When you execute this command, the existing monitoring object database is deleted and a new monitoring object database is created.

You must terminate JP1/IM - Manager before you can create a monitoring object database.

Make sure that you execute this command if you use any Central Scope functions.

Format

```
jcsdbsetup [-h logical-host-name]
           [-f]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

`-f`

You must specify this option when there is an existing monitoring object database (if this option is omitted in such a case, an error results). If there is no existing monitoring object database, you can omit this option.

When this option is specified and there is a monitoring object database, the command displays the confirmation message `Database files are existed. Delete these files? [y/n]`. Entering `Y` and then pressing the **Enter** key will cause the existing monitoring object database to be deleted and a new monitoring object database to be created. If there is no existing monitoring object database, the command will create a new monitoring object database without displaying the confirmation message.

Return values

0	Normal termination
1	Logical host name is invalid

2	Argument error
4	No permission to execute the command
10	Setup has not been completed
12	Insufficient memory
13	Insufficient disk capacity
20	Database already exists
42	Another command or request is running
99	Other error

jcshostsexport

Function

This command acquires host information from the host information database. When this command is executed, it loads host information from the host information database and stores it in a specified host information file (if no host information file name is specified, the host information is output to standard output).

You can use this command when the Central Scope functions are enabled.

Format

```
jcshostsexport [-h logical-host-name] > host-information-file-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

host-information-file-name

Specifies the name of the file in which the host information is to be stored.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1scope`
  - `/`*shared-directory-name*`/jp1scope/log`

Delete /*shared-directory-name* directory and files under it. Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	Normal termination
`1`	Logical host name is invalid
`2`	Argument error
`4`	No permission to execute the command
`10`	Setup has not been completed
`11`	There is no host information database
`12`	Insufficient memory
`14`	Host information database is corrupted
`15`	Message initialization failed
`16`	Host information database is in use
`99`	Other error

jcshostsimport

Function

This command registers host information into and deletes host information from the host information database. You can apply the host information while JP1/IM - Manager is running by executing the `jco_spmd_reload` command after this command has executed. While JP1/IM - Manager is stopped, you can apply the host information by starting JP1/IM - Manager.

You can use this command when the Central Scope functions are enabled.

Format

```
jcshostsimport { { -o | -r } host-information-file-name | -d}
               [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Scope-path`\bin\`

In UNIX:

`/opt/jp1scope/bin/`

Arguments

`-r` *host-information-file-name*

Specifies the name of the file that contains the host information that is to be registered into the host information database. When the `-r` option is specified, the command deletes all host information from the existing host information database and then registers the specified host information into the database.

For details about the format of the host information file, see *Host information file (jcs_hosts)* in *Chapter 2. Definition Files*.

`-o` *host-information-file-name*

Specifies the name of the file that contains the host information that is to be registered into the host information database. When the `-o` option is specified, the command adds to the host information database the host information contained in the host information file without deleting the existing host information from the database (if an identical IP address exists, the information for that host is overwritten).

For details about the format of the host information file, see *Host information file (jcs_hosts)* in *Chapter 2. Definition Files*.

`-d`

Specifies that all the existing host information is to be completely deleted from the host information database.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed.

Notes

- Execute this command only on the active host. Make sure that the shared disk is mounted when the command executes.
- Do not execute this command on the standby host.

  If you execute with standby host in UNIX / Linux, an unwanted directory named `/`*shared-directory-name* is created under the root directory of standby host local disk, and further unwanted directory and Files are created under that directory as follows.

  - `/`*shared-directory-name*`/jp1scope`
  - `/`*shared-directory-name*`/jp1scope/log`

  Delete `/`*shared-directory-name* directory and files under it. Delete these unwanted directory and files, they will never to be used. To prevent from mistakenly deleting the directory from shared directory, make sure that shared disk is not mounted on standby host before deleting the directory.

Return values

`0`	Normal termination
`1`	Logical host name is invalid
`2`	Argument error
`3`	File name is invalid
`4`	No permission to execute the command
`5`	Syntax error in the specified host information file
`6`	No permission to access the specified host information file
`10`	Setup has not been completed
`11`	There is no host information database
`12`	Insufficient memory
`13`	Insufficient disk capacity
`14`	Host information database is corrupted
`15`	Message initialization failed
`16`	Host information database is in use
`99`	Other error

jim_log.bat (Windows only)

Function

This is a tool for collecting data in the event of a failure in JP1/IM - Manager or JP1/IM - View. The data collected by this tool includes maintenance information for JP1/IM - Manager, JP1/IM - View, and JP1/Base, system information from the OS, and integrated trace logs.

This tool is a batch file, which cannot be customized by the user.

When you execute this tool, the target folders or files used for data collection are classified into primary and secondary data categories and the collected data is stored directly under the specified data storage folder.

The primary data is collected for such purposes as identifying a failure and investigating the causes of minor failures. It consists of the minimum amount of logs and settings files. The secondary data provides the detailed information needed for an in-depth investigation of a failure. It consists of such data as the Windows event log and the JP1/Base event database.

If you execute `jim_log.bat` while a thread dump of JP1/IM - Manager (Central Console) or JP1/IM - View is available, the tool displays the `KAVB8946-I` message asking whether you want to delete the thread dump. If you enter `y`, the tool deletes the thread dump.

If necessary, use a program such as a compression tool to compress the collected data.

For details about the data that can be collected by this tool, see *12.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

If you are using the intelligent integrated management database, you can also collect data about the intelligent integrated management database#.

#

The logs of the intelligent integrated management database itself are excluded from the collection of this tool. If the case corresponds to described in *12.3.1(1)(b) JP1 information* in the *JP1/Integrated Management 3 - Administration Guide*, collect the logs manually.

If you do not want to obtain maintenance information of the intelligent integrated management database, execute this tool with specifying `-i` option.

The following tables show the organization of folders directly under the data storage folder and the data that is stored.

Table 1–39: Organization of the internal folders for the primary data of the physical host

Folder name	Stored data
data-storage-folder`\jp1_default\imm_1st\imm`	• Data storage folder for JP1/IM - Manager • JP1/IM - Manager patch information
data-storage-folder`\jp1_default\imm_1st\imm\conf`	JP1/IM - Manager settings and definition files
data-storage-folder`\jp1_default\imm_1st\imm\log`	Log files for JP1/IM - Manager
data-storage-folder`\jp1_default\imm_1st\cons`	Data storage folder for JP1/IM - Manager (Central Console)
data-storage-folder`\jp1_default\imm_1st\cons\conf`	JP1/IM - Manager (Central Console) settings and definition files
data-storage-folder`\jp1_default\imm_1st\cons\default`	Common definition information for JP1/IM - Manager (Central Console)

Folder name	Stored data
data-storage-folder`\jp1_default\imm_1st\cons\log`	Log files for JP1/IM - Manager (Central Console)
data-storage-folder`\jp1_default\imm_1st\scope`	Data storage folder for JP1/IM - Manager (Central Scope)
data-storage-folder`\jp1_default\imm_1st\scope\conf`	JP1/IM - Manager (Central Scope) settings and definition files
data-storage-folder`\jp1_default\imm_1st\scope\default`	Common definition information for JP1/IM - Manager (Central Scope)
data-storage-folder`\jp1_default\imm_1st\scope\log`	Log files for JP1/IM - Manager (Central Scope)
data-storage-folder`\jp1_default\imm_1st\coview`	• Data storage folder for JP1/IM - View • JP1/IM - View patch information
data-storage-folder`\jp1_default\imm_1st\coview\conf`	JP1/IM - View settings and definition files
data-storage-folder`\jp1_default\imm_1st\coview\default`	Common definition information for JP1/IM - View
data-storage-folder`\jp1_default\imm_1st\coview\log`	Log files for JP1/IM - View
data-storage-folder`\jp1_default\imm_1st\imm\Patchlog_jp1imm.txt`	JP1/IM - Manager patch information
data-storage-folder`\jp1_default\imm_1st\imm\conf\tools`	JP1/IM - Manager settings and definition files
data-storage-folder`\jp1_default\imm_1st\imm\log\operationlog`	JP1/IM - Manager operation log
data-storage-folder`\jp1_default\imm_1st\imcf\conf\imcf`	IM Configuration Management settings and definition files
data-storage-folder`\jp1_default\imm_1st\imdb\conf\imdb`	IM database settings and definition files
data-storage-folder`\jp1_default\imm_1st\imcf\system\default\new\imcf`	Common definition information for IM Configuration Management
data-storage-folder`\jp1_default\imm_1st\imdb\database\imdb`	Detailed log information for the IM database
data-storage-folder`\jp1_default\imm_1st\imcf\log\imcf`	Log files for IM Configuration Management
data-storage-folder`\jp1_default\imm_1st\imdb\log\imdb`	Log files for the IM database
data-storage-folder`\jp1_default\imm_1st\base`	• Data storage folder for JP1/Base • JP1/Base patch information
data-storage-folder`\jp1_default\imm_1st\base\conf`	JP1/Base settings and definition files
data-storage-folder`\jp1_default\imm_1st\base\default`	Common definition information for JP1/Base
data-storage-folder`\jp1_default\imm_1st\base\log`	Log files for JP1/Base
data-storage-folder`\jp1_default\imm_1st\base\plugin\conf`	Settings file for JP1/Base plug-in services

Folder name	Stored data
data-storage-folder`\jp1_default\imm_1st\base\sys\tmp`	Logs and temporary files for JP1/Base
data-storage-folder`\jp1_default\imm_1st\oslog`	OS log information
data-storage-folder`\jp1_default\imm_1st\spool`	Integrated trace logs (32-bit)
data-storage-folder`\jp1_default\imm_1st\spoolx64`	Integrated trace logs (64-bit)
data-storage-folder`\jp1_default\imm_1st\imdd`	Data storage folder for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\jp1_default\imm_1st\imdd\conf`	Settings and definition files for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\jp1_default\imm_1st\imdd\log`	Log files for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\jp1_default\imm_1st\imdd\plugin`	Plug-in for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\jp1_default\imm_1st\imdd\log\suggestion`	Response action execution history file for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\jp1_default\imm_1st\imgndb\conf`	Settings and definition files for the intelligent integrated management database
data-storage-folder`\jp1_default\imm_1st\imgndb\log`	Log files for the intelligent integrated management database

Table 1–40: Organization of the internal folders for the secondary data of the physical host

Folder name	Stored data
data-storage-folder`\jp1_default\imm_2nd\cons`	Data storage folder for JP1/IM - Manager (Central Console)
data-storage-folder`\jp1_default\imm_2nd\cons\operation\evgen`	Correlation event generation history files for JP1/IM - Manager (Central Console)
data-storage-folder`\jp1_default\imm_2nd\cons\operation\comexclude`	Common exclusion history file and common exclusion-conditions definition history file for JP1/IM - Manager (Central Console)
data-storage-folder`\jp1_default\imm_2nd\scope`	Data storage folder for JP1/IM - Manager (Central Scope)
data-storage-folder`\jp1_default\imm_2nd\scope\database`	Database information for JP1/IM - Manager (Central Scope)
data-storage-folder`\jp1_default\imm_2nd\base`	Data storage folder for JP1/Base
data-storage-folder`\jp1_default\imm_2nd\base\log\COMMAND`	Command execution log files for JP1/Base
data-storage-folder`\jp1_default\imm_2nd\base\sys\event\servers\default`	Event database for JP1/Base
data-storage-folder`\jp1_default\imm_2nd\oslog`	Windows event log
data-storage-folder`\jp1_default\imm_2nd\imcf\data\imcf`	Data files for IM Configuration Management
data-storage-folder`\jp1_default\imm_2nd\imdb\database\imdb\imdbbackup.dat`	Windows event log Backup files of the IM database

Folder name	Stored data
data-storage-folder\jp1_default\imm_2nd\imdd\data\imdd	Data files for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder\jp1_default\imm_2nd\imgndb\database\imgndb	Data files for the intelligent integrated management database

Table 1–41: Organization of the internal folders for the primary data of the logical host

Folder name	Stored data
data-storage-folder\logical-host-name\imm_1st\cons	Data storage folder for the logical host of JP1/IM - Manager (Central Console)
data-storage-folder\logical-host-name\imm_1st\cons\conf	Logical host settings and definition files for JP1/IM - Manager (Central Console)
data-storage-folder\logical-host-name\imm_1st\cons\log	Log files for the logical host of JP1/IM - Manager (Central Console)
data-storage-folder\logical-host-name\imm_1st\scope	Data storage folder for the logical host of JP1/IM - Manager (Central Scope)
data-storage-folder\logical-host-name\imm_1st\scope\conf	Logical host settings and definition files for JP1/IM - Manager (Central Scope)
data-storage-folder\logical-host-name\imm_1st\scope\log	Log files for the logical host of JP1/IM - Manager (Central Scope)
data-storage-folder\logical-host-name\imm_1st\base	Data storage folder for the logical host of JP1/Base
data-storage-folder\logical-host-name\imm_1st\base\conf	Logical host name settings and definition files for JP1/Base
data-storage-folder\logical-host-name\imm_1st\base\event	Event server settings for the logical host of JP1/Base
data-storage-folder\logical-host-name\imm_1st\base\log	Log files for the logical host of JP1/Base
data-storage-folder\logical-host-name\imm_1st\oslog	OS log information
data-storage-folder\logical-host-name\imm_1st\imm\Patchlog_jp1imm.txt	JP1/IM - Manager patch information
data-storage-folder\logical-host-name\imm_1st\imm\log\operationlog	JP1/IM - Manager operation log
data-storage-folder\logical-host-name\imm_1st\imcf\conf\imcf	IM Configuration Management settings and definition files
data-storage-folder\logical-host-name\imm_1st\imdb\database\imdb	Detailed log information for the IM database
data-storage-folder\logical-host-name\imm_1st\imcf\log\imcf	Log files for IM Configuration Management
data-storage-folder\logical-host-name\imm_1st\imdb\log\imdb	Log files for the IM database
data-storage-folder\logical-host-name\imm_1st\imdd	Data storage folder for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder\logical-host-name\imm_1st\imdd\conf	Settings and definition files for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder\logical-host-name\imm_1st\imdd\log	Log files for JP1/IM - Manager (Intelligent Integrated Management Base)

Folder name	Stored data
data-storage-folder`\`*logical-host-name*`\imm_1st\imdd\plugin`	Plug-in for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\`*logical-host-name*`\imm_1st\imdd\log\suggestion`	Response action execution history file for JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\`*logical-host-name*`\imm_1st\imgndb\conf`	Settings and definition files for the intelligent integrated management database
data-storage-folder`\`*logical-host-name*`\imm_1st\imgndb\log`	Log files for the intelligent integrated management database

Table 1–42: Organization of the internal folders for the secondary data of the logical host

Folder name	Stored data
data-storage-folder`\`*logical-host-name*`\imm_2nd\cons`	Data storage folder for the logical host of JP1/IM - Manager (Central Console)
data-storage-folder`\`*logical-host-name*`\imm_2nd\cons\operation\evgen`	Correlation event generation history file for the logical host of JP1/IM - Manager (Central Console)
data-storage-folder`\`*logical-host-name*`\imm_2nd\cons\operation\comexclude`	Common exclusion history file and common exclusion-conditions definition history file for the logical host of JP1/IM - Manager (Central Console)
data-storage-folder`\`*logical-host-name*`\imm_2nd\scope`	Data storage folder for the logical host of JP1/IM - Manager (Central Scope)
data-storage-folder`\`*logical-host-name*`\imm_2nd\scope\database`	Database information for the logical host of JP1/IM - Manager (Central Scope)
data-storage-folder`\`*logical-host-name*`\imm_2nd\base`	Data storage folder for the logical host of JP1/Base
data-storage-folder`\`*logical-host-name*`\imm_2nd\base\log\COMMAND`	Command execution log files for the logical host of JP1/Base
data-storage-folder`\`*logical-host-name*`\imm_2nd\base\event`	Event database for the logical host of JP1/Base
data-storage-folder`\`*logical-host-name*`\imm_2nd\imcf\data\imcf`	Data files for IM Configuration Management
data-storage-folder`\`*logical-host-name*`\imm_2nd\imdb\database\imdb\imdbbackup.dat`	Backup files of the IM database
data-storage-folder`\`*logical-host-name*`\imm_2nd\imdd\data\imdd`	Data files for the logical host of JP1/IM - Manager (Intelligent Integrated Management Base)
data-storage-folder`\`*logical-host-name*`\imm_2nd\imgndb\database\imgndb`	Data files for the logical host of the intelligent integrated management database

Format

```
jim_log.bat -f data-storage-folder
            [-h logical-host-name]
            [-t]
            [-n]
            [-p]
            [-r]
            [-g]
            [-a]
            [-s]
            [-c]
```

```
              [-d]
              [-x]
              [-w]
              [-q]
              [-b]
              [-i]
```

The `-a` option is used for linking with BJEX or JP1/AS. For details about the `-a` option, see *11.5.2 jim_log.bat (Windows only)* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Execution permission

Administrator permissions (If the Windows UAC feature is enabled, the command must be executed from the administrator console.)

Storage directory

Manager-path`\tools\`

Arguments

`-f` *data-storage-folder*

Specifies the name of the folder to which the collected data is to be output, expressed as a full path or a path relative to the location where the command is executed. If the path contains a space, enclose the entire path in double-quotation marks (`"`). This option is mandatory.

If a nonexistent folder is specified, a new folder with the specified name is created. If an existing folder is specified, the contents of that existing folder are deleted and the specified folder is created.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies a logical host name and that the command is to collect data for that logical host as well as for the physical host. If this option is omitted, the command collects data for the physical host only. If you are not using a cluster system, there is no need to specify this option.

Note that this command will not use the logical host name that is set in the `JP1_HOSTNAME` environment variable. Therefore, if you use this command in a cluster system, make sure that you specify the logical host name in this option.

`-t`

Specifies that the `hosts` and `services` files are not to be collected.

`-n`

Specifies that maintenance data for JP1/Base is not to be collected.

`-p`

Specifies that the event database for JP1/Base is not to be collected.

`-r`

Specifies that the command execution log files for JP1/Base are not to be collected.

`-g`

Specifies that the correlation event generation history file is not to be collected.

`-a`

Specifies that the file for accumulated response-waiting events is not to be collected.

`-s`

Specifies that maintenance data for JP1/IM - Manager (Central Scope) is not to be collected.

`-c`

Specifies that maintenance data for IM Configuration Management is not to be collected.

`-d`

Specifies that maintenance data for the IM database is not to be collected.

This argument cannot be specified together with the `-x` option.

`-x`

Specifies that IM database backup files are to be collected.

This argument cannot be specified together with the `-d` option.

The IM database backup files are not included in the maintenance data for the IM database that is collected by default. If the IM database service is not running, the maintenance data is not collected; in such a case, start the IM database service and then re-execute the data collection tool. The backup files can be collected even when JP1/IM - Manager is running.

`-w`

Specifies that maintenance data for JP1/IM - View is not to be collected.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

`-b`

Specifies that maintenance data for Intelligent Integrated Management Base is not to be collected.

`-i`

Specifies that maintenance data for the intelligent integrated management database is not to be collected.

Notes

- This tool might collect a large amount of data. Before you execute this tool, you need to estimate the amount of disk space required and then check the capacity available on your machine. For details, see *12.4 Collecting data* in the *JP1/Integrated Management 3 - Manager Administration Guide*.
- Do not execute this tool more than once.
- If a file to be collected is not found, the tool might display a message such as `The file was not found`. However, it is not necessary to take any action.
- When you start JP1/Base or JP1/IM - Manager, it might display a message such as `Sharing violation`. However, it is not necessary to take any action.
- When you run the tool to collect the data, it places a certain amount of load on the computer (on disk I/O and other resources).
- If you send data to the support service without using this tool or send it with some of it excluded, detailed investigation may not be possible.

Return values

`0`	Normal termination
`8`	Abnormal termination

Example 1

Collect data for the physical host and for logical host `hostA` into the `D:\temp` folder:

```
jim_log.bat -f D:\temp -h hostA
```

The output result is as follows:

```
KAVB8925-I The directory does not exist. ("D:\temp\jp1_default\imm_1st")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("D:\temp\jp1_default\imm_2nd")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("D:\temp\hostA\imm_1st")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("D:\temp\hostA\imm_2nd")
           The directory will be created.
Press any key to continue...
KAVB8926-I Data acquisition processing will start.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfI
nfo.exe" command will start.
KAVB8921-I The information for JP1/IM - Manager will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8922-I The information for JP1/IM - Manager has been acquired.
KAVB8921-I The information for JP1/IM - Central Console will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8921-I The logical host (hostA) information will be acquired.
KAVB8922-I The logical host (hostA) information has been acquired.
KAVB8922-I The information for JP1/IM - Central Console has been acquired.
KAVB8921-I The information for JP1/IM - Central Scope will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8921-I The logical host (hostA) information will be acquired.
KAVB8922-I The logical host (hostA) information has been acquired.
KAVB8922-I The information for JP1/IM - Central Scope has been acquired.
KAVB8921-I The information for JP1/Base will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8921-I The logical host (hostA) information will be acquired.
KAVB8922-I The logical host (hostA) information has been acquired.
KAVB8922-I The information for JP1/Base has been acquired.
KAVB8921-I The information for JP1/IM - View will be acquired.
KAVB8922-I The information for JP1/IM - View has been acquired.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8929-I The system information will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInf
o.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInfo.exe" execution
is ended. (ERRORLEVEL=0)
KAVB8922-I The system information has been acquired.
KAVB8929-I "Watson log and crash dump" will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnI
nfo.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8922-I "Watson log and crash dump" has been acquired.
KAVB8921-I Windows Eventlog(Application) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
```

```
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(Application) has been acquired.
KAVB8921-I Windows Eventlog(System) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(System) has been acquired.
KAVB8921-I The setup.ini of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ini of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ini of JP1/IM - View will be acquired.
KAVB8922-I The setup.ini of JP1/IM - View has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - View will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - View has been acquired.
KAVB8921-I The setup.ini of JP1/Base will be acquired.
KAVB8922-I The setup.ini of JP1/Base has been acquired.
KAVB8921-I The setup.ilg of JP1/Base will be acquired.
KAVB8922-I The setup.ilg of JP1/Base has been acquired.
KAVB8921-I The integrated trace log will be acquired.
KAVB8922-I The integrated trace log has been acquired.
KAVB8921-I The integrated installer log will be acquired.
KAVB8922-I The integrated installer log has been acquired.
KAVB8921-I The installer log file will be acquired.
KAVB8922-I The installer log file has been acquired.
KAVB8921-I The hosts will be acquired.
KAVB8922-I The hosts has been acquired.
KAVB8921-I The services will be acquired.
KAVB8922-I The services has been acquired.
KAVB8921-I The registry information will be acquired.
KAVB8922-I The registry information has been acquired.
KAVB8921-I The netstat information will be acquired.
KAVB8922-I The netstat information has been acquired.
KAVB8921-I The ipconfig information will be acquired.
KAVB8922-I The ipconfig information has been acquired.
KAVB8921-I The net start information will be acquired.
KAVB8922-I The net start information has been acquired.
KAVB8921-I The set information will be acquired.
KAVB8922-I The set information has been acquired.
KAVB8918-I The data was successfully acquired.
```

Example 2

Collect data for the physical host into the nonexistent folder `D:\temp`, but do not specify the existing logical host (`hostA`):

```
jim_log.bat -f D:\temp
```

The output result is as follows:

```
KAVB8925-I The directory does not exist. ("D:\temp")
           The directory will be created.
Press any key to continue...
```

```
KAVB8925-I The directory does not exist. ("D:\temp\jp1_default\imm_1st")
           The directory will be created.
Press any key to continue...
KAVB8925-I The directory does not exist. ("D:\temp\jp1_default\imm_2nd")
           The directory will be created.
Press any key to continue...
KAVB8926-I Data acquisition processing will start.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfI
nfo.exe" command will start.
KAVB8921-I The information for JP1/IM - Manager will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8922-I The information for JP1/IM - Manager has been acquired.
KAVB8921-I The information for JP1/IM - Central Console will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8922-I The information for JP1/IM - Central Console has been acquired.
KAVB8921-I The information for JP1/IM - Central Scope will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8922-I The information for JP1/IM - Central Scope has been acquired.
KAVB8921-I The information for JP1/Base will be acquired.
KAVB8921-I The physical host information will be acquired.
KAVB8922-I The physical host information has been acquired.
KAVB8922-I The information for JP1/Base has been acquired.
KAVB8921-I The information for JP1/IM - View will be acquired.
KAVB8922-I The information for JP1/IM - View has been acquired.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetConfInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8929-I The system information will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInf
o.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetMsInfo.exe" execution
is ended. (ERRORLEVEL=0)
KAVB8922-I The system information has been acquired.
KAVB8929-I "Watson log and crash dump" will be acquired. Please wait.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnI
nfo.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetWtsnInfo.exe" executio
n is ended. (ERRORLEVEL=0)
KAVB8922-I "Watson log and crash dump" has been acquired.
KAVB8921-I Windows Eventlog(Application) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(Application) has been acquired.
KAVB8921-I Windows Eventlog(System) will be acquired.
KAVB8927-I Execution of the "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog
.exe" command will start.
KAVB8928-I "D:\Program Files\Hitachi\JP1IMM\bin\jimGetEvLog.exe" execution i
s ended. (ERRORLEVEL=0)
KAVB8922-I Windows Eventlog(System) has been acquired.
KAVB8921-I The setup.ini of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ini of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - Manager will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - Manager has been acquired.
KAVB8921-I The setup.ini of JP1/IM - View will be acquired.
```

```
KAVB8922-I The setup.ini of JP1/IM - View has been acquired.
KAVB8921-I The setup.ilg of JP1/IM - View will be acquired.
KAVB8922-I The setup.ilg of JP1/IM - View has been acquired.
KAVB8921-I The setup.ini of JP1/Base will be acquired.
KAVB8922-I The setup.ini of JP1/Base has been acquired.
KAVB8921-I The setup.ilg of JP1/Base will be acquired.
KAVB8922-I The setup.ilg of JP1/Base has been acquired.
KAVB8921-I The integrated trace log will be acquired.
KAVB8922-I The integrated trace log has been acquired.
KAVB8921-I The integrated installer log will be acquired.
KAVB8922-I The integrated installer log has been acquired.
KAVB8921-I The installer log file will be acquired.
KAVB8922-I The installer log file has been acquired.
KAVB8921-I The hosts will be acquired.
KAVB8922-I The hosts has been acquired.
KAVB8921-I The services will be acquired.
KAVB8922-I The services has been acquired.
KAVB8921-I The registry information will be acquired.
KAVB8922-I The registry information has been acquired.
KAVB8921-I The netstat information will be acquired.
KAVB8922-I The netstat information has been acquired.
KAVB8921-I The ipconfig information will be acquired.
KAVB8922-I The ipconfig information has been acquired.
KAVB8921-I The net start information will be acquired.
KAVB8922-I The net start information has been acquired.
KAVB8921-I The set information will be acquired.
KAVB8922-I The set information has been acquired.
KAVB8918-I The data was successfully acquired.
KAVB8934-I The following logical host(s) exist on this machine:
hostA
To acquire information about a logical host, execute "jim_log.bat -f output
-directory-name -h logical-hostname".
Press any key to continue...
```

jim_log.sh (UNIX only)

Function

This is a tool for collecting data in the event of a failure in JP1/IM - Manager. The data collected by this tool includes maintenance information for JP1/IM - Manager and JP1/Base, system information from the OS, and integrated trace logs.

This tool is a shell script, which cannot be customized by the user.

When you execute this tool, it classifies the target directories or files used for data collection into primary and secondary data categories, uses the `tar` command to archive the data directly under the specified data storage directory, and then uses the `compress` command to create compressed files.

The primary data is collected for such purposes as identifying a failure and investigating the causes of minor failures. It consists of the minimum amount of logs and settings files. The secondary data provides the detailed information needed for an in-depth investigation of a failure. It consists of such data as core analysis information and data from the JP1/Base event database.

In an environment where the output of core files of the systemd-core dump is enabled, from the list of core files held on the system when this tool is executed, regarding the core files output by the JP1/IM-M process, the core files in the collection-target log file directory are collected.

If you execute the `jim_log.sh` command while a core dump and a thread dump of JP1/IM - Manager (Central Console) are available, the tool displays the `KAVB8941-I` and `KAVB8942-I` messages asking whether you want to delete the core dump or the thread dump. If you enter `y` or `yes`, the tool deletes the core dump or thread dump.

For details about the data that can be collected by this tool, see *12.3 Data that needs to be collected when a problem occurs* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

If you are using the intelligent integrated management database, you can also collect data about the intelligent integrated management database#.

#

> The logs of the intelligent integrated management database itself are excluded from the collection of this tool. If the case corresponds to described in *12.3.1(2)(b) JP1 information* in the *JP1/Integrated Management 3 - Administration Guide*, collect the logs manually.

If you do not want to obtain maintenance information of the intelligent integrated management database, execute this tool with specifying `-i` option.

The following table lists and describes the compressed files containing the collected data.

Table 1–43: Compressed files containing the collected data

File name	Description
`jp1_default_imm_1st.tar.Z`	Primary data for the physical host
`jp1_default_imm_2nd.tar.Z`	Secondary data for the physical host
logical-host-name`_imm_1st.tar.Z`#	Primary data for the logical host
logical-host-name`_imm_2nd.tar.Z`#	Secondary data for the logical host

#: Created only when a logical host was specified in the `-h` option.

The compressed files are stored in the data storage directory. The following tables show the organization of the internal directories for the compressed files.

Table 1–44: Organization of the internal directories for the primary data of the physical host

Directory and file name	Stored data
`./etc/opt/jp1base`	Automated startup and stop scripts for JP1/Base
`./etc/opt/jp1base/conf`	JP1/Base settings and definition files
`./etc/opt/jp1base/default`	Common definition information for JP1/Base
`./etc/opt/jp1cons`	Automated startup and stop scripts for JP1/IM - Manager (Central Console)
`./etc/opt/jp1cons/conf`	JP1/IM - Manager (Central Console) settings and definition files
`./etc/opt/jp1cons/default`	Common definition information for JP1/IM - Manager (Central Console)
`./etc/opt/jp1imm/conf/tools`	JP1/IM - Manager settings and definition files
`./etc/opt/jp1imm/conf/imcf`	IM Configuration Management settings and definition files
`./etc/opt/jp1imm/conf/imdb`	IM database settings and definition files
`./etc/opt/jp1imm/conf/imdd`	Settings and definition files for JP1/IM - Manager (Intelligent Integrated Management Base)
`./etc/opt/jp1imm/conf/imgndb`	Settings and definition files for the intelligent integrated management database
`./etc/opt/jp1imm/plugin`	Plug - in for JP1/IM - Manager (Intelligent Integrated Management Base)
`./var/opt/jp1imm/log/suggestion`	Response action execution history file for JP1/IM - Manager (Intelligent Integrated Management Base)
`./etc/opt/jp1imm/default/imcf`	Common definition information for IM Configuration Management
`./etc/opt/jp1scope/conf`	JP1/IM - Manager (Central Scope) settings and definition files
`./etc/opt/jp1scope/default`	Common definition information for JP1/IM - Manager (Central Scope)
`./opt/jp1/hcclibcnf`	Common definition information
`./opt/jp1base`	Patch application history and patch log information for JP1/Base
`./opt/jp1base/conf`	Settings file for JP1/Base plug-in services
`./opt/jp1imm`	Patch application history and patch log information for JP1/IM - Manager
`./var/opt/jp1base/log`	Log files for JP1/Base
`./var/opt/jp1base/sys/tmp`	Logs and temporary files for JP1/Base
`./var/opt/hitachi/HNTRLib2/spool`	Integrated trace logs
`./var/opt/jp1cons/log`	Log files for JP1/IM - Manager (Central Console)
`./var/opt/jp1imm/database/imdb`	Detailed log information for the IM database
`./var/opt/jp1imm/log/imcf`	Log files for IM Configuration Management
`./var/opt/jp1imm/log/imdb`	Log files for the IM database

Directory and file name	Stored data
`./var/opt/jp1imm/log/imdd`	Log files for JP1/IM - Manager (Intelligent Integrated Management Base)
`./var/opt/jp1imm/log/imgndb`	Log files for the intelligent integrated management database
`./var/opt/jp1imm/log/_jp1_default/oslog`	OS log information
`./var/opt/jp1imm/log/_jp1_default/operationlog`	JP1/IM - Manager operation log
`./var/opt/jp1scope/log`	Log files for JP1/IM - Manager (Central Scope)

Table 1–45: Organization of the internal directories for the secondary data of the physical host

Directory and file name	Stored data
`./var/opt/jp1base/log/COMMAND`	Command execution log files for JP1/Base
`./var/opt/jp1base/sys/event/servers/default`	Event database for JP1/Base
`./var/opt/jp1cons/operation/comexclude`	Common exclusion history file and common exclusion-conditions definition history file for JP1/IM - Manager (Central Console)
`./var/opt/jp1cons/operation/evgen`	Correlation event generation history files for JP1/IM - Manager (Central Console)
`./var/opt/jp1imm/log/_jp1_default/oslog`	OS log information
`./var/opt/jp1imm/log/_jp1_default/core`	Core file
`./var/opt/jp1scope/database`	Database information for JP1/IM - Manager (Central Scope)
`./var/opt/jp1imm/data/imcf`	Data files for IM Configuration Management
`./var/opt/jp1imm/database/imdb/imdbbackup.dat`	Backup files of the IM database
`./var/opt/jp1imm/data/imdd`	Data files for JP1/IM - Manager (Intelligent Integrated Management Base)

`./tmp/.JP1_SES*`
`./usr/tmp/jp1_ses`
`./usr/lib/jp1_ses/log`
`./usr/lib/jp1_ses/sys`
`./usr/bin/jp1_ses/jp*`
`./var/opt/jp1_ses`
	Log for JP1/SES compatibility

Table 1–46: Organization of the internal directories for the primary data of the logical host

Directory and file name	Stored data
`./`*shared-disk*`/jp1base/../event`	Event server settings for the logical host of JP1/Base
`./`*shared-disk*`/jp1base/conf`	Logical host settings and definition files for JP1/Base
`./`*shared-disk*`/jp1base/log`	Log files for the logical host of JP1/Base
`./`*shared-disk*`/jp1cons/conf`	Logical host settings and definition files for JP1/IM - Manager (Central Console)

Directory and file name	Stored data
./*shared-disk*/jp1cons/log	Log files for the logical host of JP1/IM - Manager (Central Console)
./*shared-disk*/jp1scope/conf	Logical host settings and definition files for JP1/IM - Manager (Central Scope)
./*shared-disk*/jp1scope/log	Log files for the logical host of JP1/IM - Manager (Central Scope)
./var/opt/jp1imm/log/*_logical-host-name*/oslog	OS log information
./var/opt/jp1imm/log/*_logical-host-name*/operationlog	JP1/IM - Manager operation log
./*shared-disk*/jp1imm/conf/imcf	IM Configuration Management settings and definition files
./*shared-disk*/jp1imm/conf/imdd	Settings and definition files for JP1/IM - Manager (Intelligent Integrated Management Base)
./*shared-disk*/jp1imm/conf/imgndb	Settings and definition files for the intelligent integrated management database
./var/opt/jp1imm/database/imdb	Detailed log information for the IM database
./*shared-disk*/jp1imm/log/imcf	Log files for IM Configuration Management
./*shared-disk*/jp1imm/log/imdd	Log files for JP1/IM - Manager (Intelligent Integrated Management Base)
./*shared-disk*/jp1imm/log/imgndb	Log files for the intelligent integrated management database
./*shared-disk*/jp1imm/log/suggestion	Response action execution history file for JP1/IM - Manager (Intelligent Integrated Management Base)
./var/opt/jp1imm/log/imdb	Log files for the IM database

Table 1–47: Organization of the internal directories for the secondary data of the logical host

Directory and file name	Stored data
./*shared-disk*/event	Event database for the logical host of JP1/Base
./*shared-disk*/jp1base/log/COMMAND	Command execution log files for the logical host of JP1/Base
./*shared-disk*/jp1cons/operation/evgen	Correlation event generation history files for the logical host of JP1/IM - Manager (Central Console)
./*shared-disk*/jp1cons/operation/comexclude	Common exclusion history file and common exclusion-conditions definition history file for the logical host of JP1/IM - Manager (Central Console)
./*shared-disk*/jp1scope/database	Database information for the logical host of JP1/IM - Manager (Central Scope)

Directory and file name	Stored data
./var/opt/jp1imm/log/_*logical-host-name*/oslog	OS log information
./var/opt/jp1imm/log/_*logical-host-name*/core	Core file
./*shared-disk*/jp1imm/data/imcf	Data files for IM Configuration Management
./*shared-disk*/jp1imm/database/imdb/imdbbackup.dat	Backup files of the IM database
./*shared-disk*/jp1imm/data/imdd	Data files for JP1/IM - Manager (Intelligent Integrated Management Base)

Format

```
jim_log.sh -f data-storage-directory
           [-h logical-host-name]
           [-t]
           [-u]
           [-n]
           [-p]
           [-r]
           [-g]
           [-a]
           [-s]
           [-c]
           [-d]
           [-x]
           [-q]
           [-b]
           [-i]
           [directory-name-or-file-name...]
```

The `-a` option is used for linking with BJEX or JP1/AS. For details about the `-a` option, see *11.5.3 jim_log.sh (UNIX only)*in the *JP1/Integrated Management 3 - Manager Administration Guide*.

Execution permission

Superuser permissions

Storage directory

`/opt/jp1imm/tools/`

Arguments

`-f` *data-storage-directory*

Specifies the name of the directory or device to which the collected data is to be output, expressed as a full path or a path relative to the root directory. If you specify a directory name, the tool creates the files containing the collected data under that directory. If the path contains a space, enclose the entire path in double-quotation marks ("). This option is mandatory.

If a nonexistent directory is specified, a new directory with the specified name is created. If an existing directory is specified, that directory is deleted and the specified directory is created.

If a device name is specified, a write operation occurs on that device for each file that is created. If a device file name such as for a tape device is specified, the collected data is stored on the device without being compressed.

If you specify a device name and the `-q` option, the tool assumes that you have chosen `yes` for user confirmation. In such a case, you must set the device before you execute the command.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies a logical host name and that the command is to collect data for that logical host as well as for the physical host. If this option is omitted, the command collects data for the physical host only. If you are not using a cluster system, there is no need to specify this option.

Note that this command will not use the logical host name that is set in the `JP1_HOSTNAME` environment variable. Therefore, if you use this command in a cluster system, make sure that you specify the logical host name in this option.

`-t`

Specifies that the `hosts`, `services`, and `passwd` files are not to be collected.

`-u`

Specifies that core analysis information is not to be collected. The core analysis information consists of a file obtained by using the `car` command of the Seraph tool to analyze a core dump file.

`-n`

Specifies that maintenance data for JP1/Base is not to be collected.

`-p`

Specifies that the event database for JP1/Base is not to be collected.

`-r`

Specifies that the command execution log files for JP1/Base are not to be collected.

`-g`

Specifies that the correlation event generation history file is not to be collected.

`-a`

Specifies that the file for accumulated response-waiting events is not to be collected.

`-s`

Specifies that maintenance data for JP1/IM - Manager (Central Scope) is not to be collected.

`-c`

Specifies that maintenance data for IM Configuration Management is not to be collected.

`-d`

Specifies that maintenance data for the IM database is not to be collected.

This argument cannot be specified together with the `-x` option.

`-x`

Specifies that IM database backup files are to be collected.

This argument cannot be specified together with the `-d` option.

The IM database backup files are not included in the maintenance data for the IM database that is collected by default. If the IM database service is not running, the maintenance data is not collected. In such a case, start the IM database service and then re-execute the data collection tool. The backup files can be collected even when JP1/IM - Manager is running.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

`-b`

Specifies that maintenance data for Intelligent Integrated Management Base is not to be collected.

`-i`

Specifies that maintenance data for the intelligent integrated management database is not to be collected.

directory-name-or-file-name

Specifies a file or directory to be collected by the data collection tool. Specify a full path name. To specify multiple names, use the space character to separate the names.

Note that this option must be the last option specified in the command. Specify it after you have specified all the other options that you need to specify. The collected data is stored as the primary data for the physical host.

Notes

- This tool might collect a large amount of data. Before you execute this tool, you need to estimate the amount of disk space required and check the capacity available on your machine. For details, see *12.4 Collecting data* in the *JP1/Integrated Management 3 - Manager Administration Guide*.
- Do not execute this tool more than once. If it is executed multiple times, previously collected data might be overwritten or data collection might fail.
- When you run the tool to collect the data, it places a certain amount of load on the computer (on disk I/O and other resources).
- If you send data to the support service without using this tool or send it with some of it excluded, detailed investigation may not be possible.

Return values

0	Normal termination
8	Abnormal termination

Example 1

Collect data for the physical host and the logical host `hostA` into `/tmp/jp1log`:

```
jim_log.sh -f /tmp/jp1log -h hostA
```

The output result is as follows:

```
KAVB8925-I The directory does not exist. (/var/opt/jp1imm/log/_jp1_default).
           The directory will be created.
KAVB8925-I The directory does not exist. (/var/opt/jp1imm/log/_hostA).
           The directory will be created.
KAVB8926-I Data acquisition processing will start.
KAVB8921-I The physical host's first material will be acquired.
KAVB8922-I The physical host's first material has been acquired.
KAVB8921-I The physical host's second material will be acquired.
KAVB8922-I The physical host's second material has been acquired.
KAVB8921-I The logical host(hostA)'s first material will be acquired.
KAVB8922-I The logical host(hostA)'s first material has been acquired.
KAVB8921-I The logical host(hostA)'s second material will be acquired.
KAVB8922-I The logical host(hostA)'s second material has been acquired.
KAVB8918-I The data was successfully acquired.
```

Example 2

Collect data for the physical host into the nonexistent directory `/tmp/jp1log/`, but do not specify the existing logical host (`hostA`):

```
jim_log.sh -f /tmp/jp1log
```

The output result is as follows:

```
KAVB8925-I The directory does not exist. (/tmp/jp1log).
           The directory will be created.
KAVB8925-I The directory does not exist. (/var/opt/jp1imm/log/_jp1_default).
           The directory will be created.
KAVB8926-I Data acquisition processing will start.
KAVB8921-I The physical host's first material will be acquired.
KAVB8922-I The physical host's first material has been acquired.
KAVB8921-I The physical host's second material will be acquired.
KAVB8922-I The physical host's second material has been acquired.
KAVB8918-I The data was successfully acquired.
KAVB8935-I The following logical host(s) exist on this machine:
hostA
To acquire information about a logical host, execute "jim_log.sh -f output-d
irectory-name -h logical-hostname".
```

Example 3

Collect data for the physical host into the `/tmp/jp1log/` directory, which contains the `jp1_default_imm_1st.tar.Z` and `jp1_default_imm_2nd.tar` files, but do not specify the existing logical host (`hostA`):

```
jim_log.sh -f /tmp/jp1log
```

The output result is as follows (when `y` is entered for all responses):

```
KAVB8925-I The directory does not exist. (/var/opt/jp1imm/log/_jp1_default).
           The directory will be created.
KAVB8926-I Data acquisition processing will start.
KAVB8921-I The physical host's first material will be acquired.
KAVB8922-I The physical host's first material has been acquired.
KAVB8921-I The physical host's second material will be acquired.
KAVB8944-I (/tmp/jp1log/jp1_default_imm_2nd.tar.Z) already exists. Do you wa
nt to overwrite it? [yes/no]y
KAVB8922-I The physical host's second material has been acquired.
KAVB8918-I The data was successfully acquired.
KAVB8944-I (/tmp/jp1log/jp1_default_imm_1st.tar.Z) already exists. Do you wa
nt to overwrite it? [yes/no]y
KAVB8935-I The following logical host(s) exist on this machine:
hostA
To acquire information about a logical host, execute "jim_log.sh -f output-d
irectory-name -h logical-hostname".
```

jimasecret

Function

This command obfuscates the specified secret and add it to the secret management File. Added secret is read and used by JP1/IM - Agent service.

For details about the secrets that you can Setup with this command, see *3.15.10 Secret obfuscation function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Format

- To list the keys that added a secret:

```
jimasecret -list
                   [-l shared-directory]
```

- To add or update a secret specifying the key:

```
jimasecret -add
                   -key key-name
                   -s secret
                   [-l shared-directory]
```

- To delete the secret specifying the key:

```
jimasecret -rm
                   -key key-name
                   [-l shared-directory]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linux:

`/opt/jp1ima/tools/`

Arguments

`-list`

Lists the keys for the secret that you add. The secrets are not displayed.

It cannot be specified together with `-add`, or `-rm` option.

`-add`

Add a new secret by keying it.

If you specify a key that has already been added, overwrite the secret. At this time, overwriting is not checked.

You can Add up to 1,000 secrets.

If you specify this option, you must also specify `-key` and `-s` options.

Cannot be specified together with `-list` or `-rm` option.

`-rm`

Delete the secret that is already added by keying.

If a key that does not exist is specified, Error is returned.

If you specify this option, you must also specify -key option.

Cannot be specified together with `-list` or `-rm` option.

`-key` *key-name*

Specifies the *key-name* of the secret that you want to add, modify, or delete.

The characters that can be specified are 0x20 to 0x7e characters of ASCII.

The maximum length that can be specified is 1,024 characters.

The specific key format is shown below.

- Information about the manager of connection desitination:

Key for the proxy password to connect to the manager host

```
immgr.proxy_user.authentication-ID
```

For *authentication-ID*, specify the user ID specified in `immgr.proxy_user` in imagent configuration file (`jpc_imagent.json`).

- The key of initial secret to connect to the manager host:

```
immgr.initial_secret
```

- The key of client secret to connect to the manager host

```
immgr.client_secret
```

- JP1/IM agent control base

The key for registration of password of the user used for Action Execution:

```
action.user.user-name
```

Set user name user that is set to `action.username` in imagent configuration file (`jpc_imagent.json`). This is only for Windows. In Linux, it is ignored even if it is specified.

Important

Value specified in -key is not checked for correct format.

Note

Specify client secret only if you want to manually delete it.

- For Blackbox exporter:

- Key to add password of the proxy authentication:

```
Blackbox.module-name.proxy_user.authentication-ID
```

For the *module-name*, specify the module name specified for Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`).

For *authentication-ID*, specify the user ID specified for `proxy_user` in Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`)

- Keys used to Add Password of the monitored Web Server:

```
Blackbox.module-name.basic_auth.authentication-ID
```

For the *module-name*, specify the module name specified for Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`).

For *authentication-ID*, specify the user ID specified for `basic_auth.username` in Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`)

- Key to add Bearer token of the monitored Web Server:

```
Blackbox.module-name.bearer_token
```

For the *module-name*, specify the module name specified for Blackbox exporter configuration file (`jpc_blackbox_exporter.yml`).

- For Primitor

- Keys used to add client secret of the Resource Discovery:

```
Promitor.resource_discovery.env.AUTH_APPKEY
```

- Key to add client secret key of the Scraper:

```
Promitor.scraper.env.AUTH_APPKEY
```

- For OracleDB exporter

There are two types of keys for registering a password for connecting to OracleDB:

- Password-key to connect to OracleDB (type of specifying the username)

  `OracleDB.user.`*user-name*

  - *username*

  Specifies the username that is set in the environment-variable `DATA_SOURCE_NAME`. Make sure to match the case.

- Password-key to connect to OracleDB (type of specifying the host name, listener service name, and username)

  `OracleDB.host.`*hostname*`.listener.`*listener-service-name*`.user.`*username*

  - *hostname*

  Specifies the hostname of OracleDB server for `DATA_SOURCE_NAME`. Make sure to match the case.

  - *listener-service-name*

  Specifies the service name of the environment-variable `DATA_SOURCE_NAME`. Make sure to match the case.

  - *username*

  Specifies the username that is set in the environment-variable `DATA_SOURCE_NAME`. Make sure to match the case.

Typically, you use the key which is the "type of specifying the username".

If more than one user with the same username exists and a different password is set, you must set a password for each OracleDB host/service using the "type of specifying the host name, listener service name, and username".

OracleDB exporter retrieves the values of the hostname, listener service name, and username from the values of the environment variable `DATA_SOURCE_NAME`. Search for a registered password by configuring the key in the "type of specifying the username" or the "type of specifying the host name, listener service name, and username". If the password could be retrieved in both formats, use the key "type of specifying the host name, listener service name, and username".

`-s` *secret*

Specifies the secret (Password) to be added or updated.

The characters that can be specified are 0x20 to 0x7e characters of ASCII.

The maximum length that can be specified is 1,024 characters.

`-l` *shared-directory*

For a Logical host environment, specify Logical host shared directory.

Specify a relative or absolute path.

The length of the path can be up to 63 bytes.

Character types are not checked.

Notes

The Value specified in `-key` is not checked for correct format.

Return values

0	Normal termination
1	Abnormal termination (user-caused Error)
2	Abnormal termination (miscellaneous Error)

Log output

- Output destination

  - In Windows:

  Agent-path`\logs\tools\`

  - In Linux:

  `/opt/jp1ima/logs/tools/`

Example

- To add a secret:

```
> jimasecret -add -key Blackbox.http1.proxy_user.p-user01 -s password01
```

- To delete a secret:

```
> jimasecret -rm -key Blackbox.http1.proxy _user.p-user01
```

- To list the keys that have been added

```
> jimasecret -list
Blackbox.http1.proxy_user.p-user01
Blackbox.http1.basic_auth.w-user01
immgr.proxy_user.user01
```

jimasetup

Function

This command performs the default Setup of JP1/IM - Agent.

Format

```
jimasetup { phost | container }
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linux:

`/opt/jp1ima/tools/`

Arguments

`phost`

If this option is specified when operating in physical host, it performs the initial Setup for operating in Physical host.

If you installed JP1/IM - Agent in a normal host deployment, the installer Execute `jimasetup phost` command.

If you created an AWS/EC2 virtual machine image, ensure that you Execute this command with `phost` optional specification from Auto Scaling scripting of AWS/EC2 before starting the service.

Cannot be specified together with `container` option.

`container`

If you created a container image, make sure that you execute this command with `container` optional specification from the scripts that the container execute before you start the service.

Cannot be specified together with `phost` option.

Return values

0	Normal termination
1	Abnormal termination

Log output

- Output destination

  - In Windows:

  Agent-path`\logs\tools\`

  - In Linux:

  `/opt/jp1ima/logs/tools/`

Example

- Sample scripting specifications for AWS/EC2's Auto Scaling

  - In Windows:

```
<script>
Agent-path\tools\jimasetup phost
Agent-path\tools\jpc_service_start -s all
</script>
```

  - In Linux:

```
#!/bin/sh
/opt/jp1ima/tools/jimasetup phost
/opt/jp1ima/tools/jpc_service_start -s all
```

- Sample specifications in scripts container executes

  - In Linux:

```
#!/bin/bash
/opt/jp1ima/tools/jimasetup container#1
exec /usr/local/bin/supervisord -c /opt/supervisord.conf#2
```

  #1: Execute of initial setting command with `container` option.

  #2: Execute the service management tools.

Notes

- Do not execute this command multiple times at the same time. If you execute multiple times at the same time, even if the command terminates with normal, the result may be incorrect.
- This command must be executed on status where all JP1/IM - Agent services are down. If you execute the command in a status JP1/IM - Agent services are running, File that you are updating might become locked and fail to update.
- Be sure to execute this command with a status that does not have a defined file open, such as in a text editor. Updating file may fail if you execute the command when definition File is open, such as with a text editor.

jimdbbackup

Function

This command backs up the IM database. The following describes the purposes of making such a backup and the types of data that can be acquired.

Backup for error recovery

You must back up the database periodically in order to recover the database in the event of a database failure. The database backup targets are the integrated monitoring database area, the IM Configuration Management database area, and the system database areas.

Backup for expansion

When you are preparing to expand the size of the database, you must temporarily back up the database's data. The database backup targets are the integrated monitoring database area and the IM Configuration Management database area.

Format

```
jimdbbackup -o backup-file-name
            -m {MAINT|EXPAND}
              [-h logical-host-name]
              [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-o` *backup-file-name*

Specifies the absolute path name of the file to which the database is to be backed up. You must specify a logical drive or a backup file. This option is mandatory.

An error results if you specify a network drive, a UNC path, or a Windows reserved device file. If the specified backup file already exists, the existing file will be overwritten.

Make sure that the value you specify for *backup-file-name* includes a file path. The characters permitted for the file name are alphanumeric characters, the underscore (_), dot (`.`), hash mark (`#`), and at mark (`@`). The character set also depends on the OS. If the name contains a space or a parenthesis (`(` or `)`), the entire name must be enclosed in double-quotation marks (`"`). In Windows, the backup file name when `MAINT` is specified must be in all lowercase letters. The maximum length of the file name depends on OS limitations.

If the directory for storing the specified backup file is not found, command execution fails. Make sure that you create the directory before you execute the command.

`-m {MAINT|EXPAND}`

Specifies the database backup format. The permitted characters are uppercase letters. This option is mandatory.

- `MAINT`: Specifies a backup for error recovery
- `EXPAND`: Specifies a backup for expansion

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command backs up the database that corresponds to the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that this logical host name cannot be `JP1_DEFAULT`. In addition, the logical host name is case sensitive.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

0	Backup terminated normally
1	Backup terminated abnormally

Notes

- Before you execute this command, make sure that the execution conditions for the `jimdbrecovery` command are satisfied.
- If you execute another JP1/IM - Manager command or start a JP1/IM - Manager service while this command is executing, execution may fail because this command places the database in the mode that disables referencing and updating.
- While this command is executing, do not press **Ctrl** +**C** or **Ctrl** + **Break**. Because the command executes backup processing in the background, the backup processing will continue even though **Ctrl** +**C** or **Ctrl** + **Break** is pressed. If you press **Ctrl** +**C** or **Ctrl** + **Break** and then immediately attempt to execute another JP1/IM - Manager command or start a JP1/IM - Manager service, execution of the requested command or startup of the requested service may fail.

  If you have canceled command execution by pressing **Ctrl** + **C** or **Ctrl** + **Break**, first make sure that the following process is not executing, and then re-execute the command:

  - `pdcopy` process if you are performing a backup for error recovery
  - `pdrorg` process if you are performing a backup for expansion
- The `jimdbbackup` command creates a backup file during execution. In the case of a backup for expansion or a backup for error recovery, the amount of free space that is needed on the drive where the backup file is to be output is about 2 gigabytes for a small database, about 15 gigabytes for a medium-sized database, and about 50 gigabytes for a large database.
- When the IM database is used, JP1/IM - Manager must not be running.
- In Windows, the IM database (JP1/IM3-Manager DB Server) must be running, and the cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) must be stopped.
- A backup file for recovery cannot be distinguished from a backup file for expansion. We recommend that you name the backup files so that you can distinguish between the types of backup files.

- At the time a backup file is output, it is in a status in which any user can access it. We recommend that immediately after you have made a backup, you change the access permissions or move the file to a protected location so that unauthorized users cannot access it.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.
- If you execute a disaster recovery backup, also consider backing up intelligent integrated management database.

jimdbreclaim

Function

This command releases free area (free page area) in the IM Configuration Management database.

If you delete a large number of hosts in the IM Configuration Management database, part of the area that was used to store that data might become used free area. This command changes used free area into unused free area so that it can be reused.

You can execute this command during operations without having to stop JP1/IM - Manager Service.

Format

```
jimdbreclaim [-h logical-host-name]
             [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command releases free area in the IM Configuration Management database for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that `JP1_DEFAULT` cannot be specified for the logical host name. In addition, the logical host name is case sensitive.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

0	Normal termination
1	Abnormal termination

Notes

- There is no need to execute this command unless you plan to repeatedly add or delete a large number of hosts in the IM Configuration Management database.

- If you execute another JP1/IM - Manager command while this command is executing, execution of the other command may fail.
- Because CPU load is high during execution of this command, we recommend that you execute it during a time when referencing and updating operations are at a minimum, such as at night.
- If you cancel this command's processing by pressing **Ctrl** + **C** or **Ctrl** + **Break**, release of free area in the database may fail. Before you re-execute the command, check that neither the `pdreclaim` process nor the `pdrorg` process is running. If either of these processes is running, wait a while and then check again.
- Do not stop the database service while this command is executing.

  If you have stopped the database service during execution of this command, you must start the database service and then re-execute the command.
- In Windows, the IM database service *JP1/IM3-Manager DB Server* must be running.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jimdbrecovery

Function

This command recovers a database from its backup. The command can recover the following types of data:

`Recovery for error recovery`

In the event of a database failure, the command recovers the database from backup data that was acquired previously.

`Recovery for expansion`

Before you expand the size of a database, temporarily back up the data.

Format

```
jimdbrecovery -i backup-file-name
              -m {MAINT|EXPAND}
              [-h logical-host-name]
              [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-i` *backup-file-name*

Specifies the absolute path name of the file to which the database was backed up by the `jimdbbackup` command. The characters permitted for the file name are alphanumeric characters, the underscore (_), dot (`.`), hash mark (`#`), and at mark (`@`). You must specify a logical drive for the backup file. This option is mandatory.

An error results if you specify a network drive, a UNC path, or a Windows reserved device file.

`-m {MAINT|EXPAND}`

Specifies the database recovery format. The permitted characters are uppercase letters. This option is mandatory.

- `MAINT`: Specifies recovery for error recovery
- `EXPAND`: Specifies recovery for expansion

When you execute recovery for error recovery, specify the backup file that was acquired by a backup for error recovery; when you execute recovery for expansion, specify the backup file that was acquired by a backup for expansion. An error results if the specified argument does not match the type of backup file.

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command recovers the database that corresponds to the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that `JP1_DEFAULT` cannot be specified for the logical host name. In addition, the logical host name is case sensitive.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

`0`	Recovery terminated normally
`1`	Recovery terminated abnormally

Notes

- When you execute the `jimdbrecovery` command to recover backup data acquired by the `jimdbbackup` command, use the same OS that was used to make the backup. If the backup is recovered to a database under a different OS, the integrity of the operation cannot be guaranteed.
- If you execute another JP1/IM - Manager command or start a JP1/IM - Manager service while this command is executing, the requested execution might fail because this command places the database in the mode that disables referencing and updating.
- While this command is executing, do not press **Ctrl** +**C** or **Ctrl** + **Break**. Because the command executes recovery processing in the background, the recovery processing will continue even though **Ctrl** +**C** or **Ctrl** + **Break** is pressed. If you press **Ctrl** +**C** or **Ctrl** + **Break** and then immediately attempt to execute another JP1/IM - Manager command or start a JP1/IM - Manager service, execution of the requested command or startup of the requested service might fail.

  If you have canceled command execution by pressing **Ctrl** +**C** or **Ctrl** + **Break** during error recovery processing, make sure that the `pdrstr` process is not running before you restart JP1/IM - Manager. If you have canceled command execution by pressing **Ctrl** +**C** or **Ctrl** + **Break** during a recovery for expansion, make sure that the `pdrorg` process is not running before you start another command or a JP1/IM - Manager service.
- This command creates a temporary file during execution. In the case of a recovery for expansion, the amount of free space needed on the drive where the IM database is to be installed is about 1 gigabyte for a small or medium-sized database, and about 4 gigabytes for a large database. In the case of a recovery for error recovery, the amount of free space needed on the drive can vary from about 5 to 50 megabytes, regardless of the database size.
- When you execute a recovery for error recovery, the database storage directory used to execute the backup for error recovery must be the same as the database storage directory used to execute the recovery for error recovery.
- When you execute a recovery for expansion, the storage space must be larger than when the backup for expansion was executed.
- Recovery for expansion might fail if the available capacity is the same as for the backup for expansion. If this occurs, set up the database again and then, with the database free of data, recover the database.
- When the IM database is used, JP1/IM - Manager must not be running.
- In Windows, the IM database (JP1/IM3-Manager DB Server) must be running and the cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) must be stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.

- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.
- If you execute a disaster recovery backup, also consider backing up intelligent integrated management database.

jimdbrorg

Function

This command reorganizes fragmented free space in the IM Configuration Management database. Free space in use is released by reorganization. Therefore, you do not need to execute the `jimdbreclaim` command many times.

When you perform maintenance of JP1/IM - Manager, you can also resolve low data storage efficiency caused by fragmentation by executing database reorganization.

Format

```
jimdbrorg [-h logical-host-name]
          [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command reorganizes the database for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that this logical host name cannot be `JP1_DEFAULT`. In addition, the logical host name is case sensitive.

`-q`

Specifies that the command is to be executed without requesting confirmation from the user.

Return values

0	Reorganization terminated normally
1	Reorganization terminated abnormally

Notes

- If you execute another JP1/IM - Manager command or start a JP1/IM - Manager service while this command is executing, the requested execution might fail.

- While this command is executing, do not press **Ctrl** +**C** or **Ctrl** + **Break**. Because the command executes database reorganization processing in the background, the database reorganization processing will continue even though **Ctrl** +**C** or **Ctrl** + **Break** is pressed. If you press **Ctrl** +**C** or **Ctrl** + **Break** and then immediately attempt to execute another JP1/IM - Manager command or start a JP1/IM - Manager service, execution of the requested command or startup of the requested service may fail.

  If you have canceled command execution by pressing **Ctrl** +**C** or **Ctrl** + **Break**, you must use a method such as the Windows Task Manager to make sure that the `pdrorg` process is not running before you execute another JP1/IM - Manager command or use JP1/IM - Manager. If the `pdrorg` process is running, wait until it terminates before executing another JP1/IM - Manager command or using JP1/IM - Manager.
- We recommend that you make a backup for error recovery before and after you execute this command.
- This command creates a temporary file during execution. For this reason, the amount of free space needed on the drive where the IM database is to be installed is about 1 gigabyte for a small or medium-sized database and about 4 gigabytes for a large database.
- When the IM database is used, JP1/IM - Manager must not be running.
- In Windows, the IM database (JP1/IM3-Manager DB Server) must be running and the cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*) must be stopped.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jimdbstatus

Function

This command checks the operating status of the IM database, such as running or stopped.

Format

```
jimdbstatus [-h logical-host-name]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command then checks the operating status of the IM database for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that the logical host name is case sensitive.

Return values

`0`	IM database is running
`1`	`jimdbstatus` command terminated abnormally
`4`	IM database is engaged in startup or termination processing
`8`	Database has been terminated (IM database restart processing was canceled and the IM database became unstable)
`12`	IM database was terminated (normal termination status)
`16`	IM database has not been started (applicable to Windows)
`20`	IM database has not been set up

Notes

Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jimdbstop

Function

This command terminates the IM database. Use this command to set the termination command with the start sequence control function of JP1/Base.

If the IM database is in restart canceled status, you can forcibly terminate it by executing this command with the `-f` option specified.

Format

```
jimdbstop [-h logical-host-name]
          [-f]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command then stops the IM database for the specified logical host. If this option is omitted, the logical host name specified in the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you are not using a cluster system, specification of this option is not needed. Note that the logical host name is case sensitive.

`-f`

Specifies that the IM database is to be terminated forcibly.

Return values

`0`	Normal termination
`1`	Abnormal termination
`4`	IM database is engaged in startup or termination processing
`8`	Database has been terminated (IM database restart processing was canceled and the IM database became unstable)
`12`	IM database was terminated (normal termination status)
`20`	IM database has not been set up

Notes

- If you cancel processing by pressing **Ctrl** + **C** or **Ctrl** + **Break**, termination of the IM database might fail. If you re-execute the command in such a case, first make sure that the `pdstop` process is not running. If the `pdstop` process is running, wait a while and then check again.
- JP1/IM - Manager must not be running while the IM database is being used.
- If you are using JP1/IM - MO, the JP1/IM - Message Optimizer service of JP1/IM - MO on the connection source must be stopped.
- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

jimdbupdate

Function

This command updates an IM database that has already been set up. Execute this command after upgrading JP1/IM - Manager.

Format

```
jimdbupdate [-h logical-host-name] [-i] [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imdb\`

In UNIX:

`/opt/jp1imm/bin/imdb/`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the name of the logical host where this command is to be executed. Execution of the command updates the IM database for the specified logical host. If you do not use a cluster system, specification of this option is not needed. Note that `JP1_DEFAULT` cannot be specified for the logical host name. In addition, the logical host name is case sensitive. For the logical host name, specify a logical host name set in JP1/Base in the correct form, especially case.

`-i`

Specify this option to update the IM database. If this option is omitted, a message asking whether the IM database needs to be updated is displayed.

`-q`

Specify this option to execute the command without requiring user confirmation.

Return values

`0`	Normal termination
`1`	Abnormal termination

Notes

- Before executing this command, make sure that the following execution conditions for this command are satisfied.

  Execution conditions

  - When this command is executed on the active server, the shared disk must be online and the logical host name must be able to be resolved.

    - In Windows, the IM database must be started.

      For a physical host:

      - JP1/IM3-Manager DB Server

      For a logical host:

      - JP1/IM3-Manager DB Server_*logical-host-name*

      In addition, the JP1/IM - Manager service and the cluster service for the IM database indicated below must be stopped. Note, however, that if the integrated monitoring database and the IM configuration management database are not used, it is not necessary to stop the JP1/IM - Manager service.

      For a physical host:

      - JP1/IM - Manager service (JP1/IM3-Manager)

      - Cluster service for the IM database (JP1/IM3-Manager DB Cluster Service)

      For a logical host:

      - JP1/IM - Manager service (JP1/IM3-Manager_*logical-host-name*)

      - Cluster service for the IM database (JP1/IM3-Manager DB Cluster Service_*logical-host-name*)

    - In UNIX, the JP1/IM - Manager service must be stopped. Note, however, that if the integrated monitoring database and the IM configuration management database are not used, it is not necessary to stop the JP1/IM - Manager service.

- If the command is stopped during execution by pressing the **Ctrl** and **C** keys or the **Ctrl** and **Break** keys, re-execute the command after making sure that the `pdeinstall` process is not being executed.

- After executing the `jimdbupdate` command, you will not be able to recover the expansion backup from the previous execution of the `jimdbupdate` command. We recommend that you make another expansion backup after executing the `jimdbupdate` command.

- After executing the command, do not attempt to recover backup data from the existing IM database that was acquired before this command was executed. We recommend that you use the `jimdbbackup` command to make another backup after executing this command.

- During execution of the `jimdbupdate` command, do not execute `jimdbstatus` or other commands related to the IM database. If you do, you might not be able to uninstall the IM database.

- Before executing the command in Windows, in case of existing the Application Experience service, make sure that the startup type of the Application Experience service is not set to **Disabled**.

- If you are upgrading JP1/IM - Manager from version earlier than 13-00 to 13-00 or later and then execute `jimdbupdate` command, note the following:

    - After September 29, 2034, do not execute `jimdbupdate` command. Perform manual uninstallation and new setup of IM database.

  For Windows, also note the following:

    - During command execute, do not use the **Ctrl** + **C** keys or the **Ctrl** + **Break** keys to abort the process. If you cancel, you may need to Redo JP1/IM - Manager version upgrade.

    - When updating IM database, close the application that locks File of IM database. If they are operating, updating may fail and redo of JP1/IM - Manager version upgrade may be required. For antivirus software, this step is required if IM database's install directory and data storage directory are not excluded from checking.

    - If IM database update fails and KNAN11215-E message is output, follow the instructions in *12.5.3(69) What to do if updating IM database with jimdbupdate command fails and a KNAN11215-E message is displayed* in the *JP1/Integrated Management 3 - Manager Administration Guide*.

  For Linux, also note the following:

    - Execute the command with Status whose SELinux is disabled.

jimgndbbackup

Function

This command backs up intelligent integrated management database.

The purpose of backup and the types of data that can be acquired are shown below.

Backup for disaster recovery

Backs up your data regularly to recover your database in the event of a database failure. The backed up areas are Trend data Management Database space, Integrated agent host Administration Database space, Dashboard Management Database space, and Response Action results management database space in the database.

Migration backup

Backs up the data to migrate the definition information in the database when migrating JP1/IM - Manager to another host. The backed up areas are Trend data Management Database space, Dashboard Management Database space, and Integrated agent host Administration Database space in the database.

The following shows Execute conditions for this command:

- There is sufficient free space on the destination drive to store the backup file to be created when this command is run.

  You must have at least as much free space as the data files for the Intelligent Integrated Management database. For details about the data files for the Intelligent Integrated Management database, see *Data file storage of the Intelligent Integrated Management database* section of *2.7.1(1)(d) Where related files are stored* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
- Stopping the following services:
  - JP1/IM3-Manager
  - JP1/IM3-Manager Intelligent Integrated DB Server
  - JP1/IM3-Manager Trend Data Management Service
- Stopping the following services when using cluster systems:
  - JP1/IM3-Manager_*logical-host-name*
  - JP1/IM3-Manager Intelligent Integrated DB Server_*logical-host-name*
  - JP1/IM3-Manager Trend Data Management Service_*logical-host-name*
- If this command is run with the `MAINT` option for argument `-m`, a backup of the IM database must have been taken using the `jimdbbackup` command (with the `MAINT` option specified for the `-m` argument).

Format

```
jimgndbbackup -o backup-filename
              -m {MAINT|TRANSF}
              [-h logical-hostname]
              [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In UNIX:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-o` *backup-filename*

Specifies the absolute pathname of file to which the database to be backed up is to be exported. For the backup file, specify the local drive. This option cannot be omitted.

Error if a network drive is specified, UNC path is specified, and reserved device File is specified in Windows. If the specified backup file already exists, it is overwritten.

The *backup-filename* must include file pathname. The characters that can be used are alphanumeric characters, underscore "`_`", dot "`.`", sharp "`#`" and at sign "`@`". Characters depend on OS and must be enclosed in double quotes if they contain single-byte spaces or parentheses "`(`", "`)`". Also, the maximum length of a File is subject to OS limitations.

`-m {MAINT|TRANSF}`

Specifies the database backup format. Half-width capital alphabet. This option cannot be omitted.

- `MAINT`: Execute the backup for disaster recovery.
- `TRANSF`: Execute the backup for migration.

`-h` *logical-hostname*

Specifies Logical host name of the host that Execute the command when operating in a cluster system. Backs up Intelligent Integrated Management Database corresponding to the specified Logical host. If this option is omitted, Logical host named in the environment variable `JP1_HOSTNAME` is assumed. If `JP1_HOSTNAME` is not specified, Physical host is assumed. If you are not using a cluster system, you do not need to specify it. Note that `JP1_DEFAULT` cannot be specified in a Logical host.

`-q`

Specifies when you execute the command without user-confirmation.

Return values

0	The backup terminated normally
1	The backup terminated abnormally
3	Canceled by user (if you enter `N/n` in KNAN12009-Q Message and Stopped the operation)

Notes

- Before you Execute this command, make sure that Execute conditions for this command and `jimgndbrestore` command are met.
- Do not start services or execute commands of other JP1/IM - Manager or JP1/IM - Agent while this command is working, Execute may fail because this command changes the database to read/write disabled mode.
- Do not press the **Ctrl** + **C** keys or the **Ctrl** + **Break** keys while this command is working. To execute the backup in the background, pressing **Ctrl** + **C** keys or **Ctrl** +**Break** keys will not stop the backup process. If you immediately start a Execute a command or start service for another JP1/IM - Manager or JP1/IM - Agent after pressing **Ctrl** + **C** keys or **Ctrl** + **Break** keys, execute or service for those commands may fail.

- If the **Ctrl** + **C** keys or the **Ctrl** + **Break** keys are used to abort the process while commands are working, the process is turned Stopped, but output Message may be corrupted.
- Because the backup file cannot be distinguished between disaster recovery and migration, we recommend that you specify a distinguishable character for each File.

  The access permissions for the backup file are printed in Status that the user can access. After making a backup, we recommend that you change the access permissions or move them to a location where users cannot access them.
- You cannot execute this command in multiple execution or concurrently with Intelligent Integrated Management Database operation commands. For details about Intelligent Integrated Management Database operation command multiplexing execute, see About multiple execution of the commands related to the Intelligent Integrated Management Database.

jimgndbrestore

Function

This command recovers Intelligent Integrated Management Database that was saved as a backup. The following are the types of data that can be recovered:

Disaster recovery

When a database failure occurs, the database is recovered using the backup data that is regularly acquired.

Migration recovery

When you migrate a JP1/IM - Manager to another host, you use the backed-up data to migrate the database.

The following shows Execute conditions for this command:

- Stopping the following services:
  - JP1/IM3-Manager
  - JP1/IM3-Manager Intelligent Integrated DB Server
  - JP1/IM3-Manager Trend Data Management Service
- Stopping the following services when using cluster systems:
  - JP1/IM3-Manager_*logical-host-name*
  - JP1/IM3-Manager Intelligent Integrated DB Server_*logical-host-name*
  - JP1/IM3-Manager Trend Data Management Service_*logical-host-name*
- If this command is run with the `MAINT` option for argument `-m`, the IM database must have been recovered using the `jimdbrecovery` command (with the `MAINT` option specified for the `-m` argument).
- Intelligent Integrated Management Database has been re-constructed.

Format

```
jimgndbrestore -i backup-filename
                -m {MAINT|TRANSF}
               [-h logical-hostname]
               [-q]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In UNIX:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-i` *backup-filename*

Specifies the absolute pathname of File of the database that was backed up using `jimgndbbackup` command. Characters that can be used in File are alphanumeric characters and underscores (`_`), dots (`.`), sharps (`#`), and at signs (`@`). For the backup file, specify the local drive. This option cannot be omitted.

Error if a network drive is specified, UNC path is specified, and reserved device File is specified in Windows.

`-m {MAINT|TRANSF}`

Specifies the database recovery format. Characters that can be specified are uppercase single-byte characters. This option cannot be omitted.

- `MAINT`: Execute the disaster recovery.
- `TRANSF`: Execute the recovery for migration.

When you execute disaster recovery, specify the backup file that was collected in the backup for disaster recovery. When you execute the recovery for migration, specify the backup file that was collected in the backup for migration.

`-h` *logical-hostname*

Specifies logical host name of the host that execute the command when operating in a cluster system. The database is recovered for the specified logical host. If this option is omitted, logical host named in the environment variable `JP1_HOSTNAME` is assumed. If `JP1_HOSTNAME` is not specified, Physical host is assumed. If you are not using a cluster system, you do not need to specify it. Note that `JP1_DEFAULT` cannot be specified in a logical host.

`-q`

Specifies when you execute the command without user-confirmation.

Return values

0	The recovery terminated normally
1	The recovery terminated abnormally
3	Canceled by user (if you enter `N/n` in KNAN12009-Q Message and Stopped the operation)

Notes

- Before you Execute this command, make sure that Execute conditions for this command and `jimgndbbackup` command are met.
- Recovering the database may cause data inconsistency between the database and JP1/IM-Agent. To prevent the data inconsistency, stop JP1/IM-Agent before recovering the database.
- This command recovers only the data in the database. To prevent data inconsistency between backup data and the data added after the backup has been taken, you must first set up the database again before recovering the database. If data inconsistency occurs, the impact can be diverse, and it is difficult to later discover the data inconsistency. Therefore, be sure to set up the database again before performing a recovery.
- While this command is working, do not start service or any other commands of JP1/IM - Manager or JP1/IM - Agent. This command might fail because this command changes the database-browsing/updating state to prohibited.
- Do not press the **Ctrl** + **C** keys or the **Ctrl** + **Break** keys while this command is working. To execute the backup in the background, pressing **Ctrl** + **C** keys or **Ctrl** + **Break** keys will not stop the backup process. If you immediately execute a command or start service for another JP1/IM - Manager or JP1/IM - Agent after pressing **Ctrl** + **C** keys or **Ctrl** + **Break** keys, execute or service for those commands may fail.
- If the **Ctrl** + **C** keys or the **Ctrl** + **Break** keys are used to abort the process while this command is working, the process is turned Stopped, but the output message may be corrupted.

- Because the recovery files are indistinguishable for disaster recovery and migration, we recommend that you specify a distinguishable character for each File.

  The access permission for the recovery file is printed in Status that the user can access. After acquiring recovery, we recommend that you change the access permissions or move them to a location where users cannot access them.

- You cannot execute this command in multiple execution or concurrently with Intelligent Integrated Management Database operation commands. For details about Intelligent Integrated Management Database operation command multiplexing execute, see About multiple execution of the commands related to the Intelligent Integrated Management Database.

jimgndbsetup

Function

Set up (install and build databases) Intelligent Integrated Management Database and Trend Data Management Services.

Also, if set up already, check and modify Setup of the database.

Format

```
jimgndbsetup  {-f setup-information-file-name
                [-h logical-host-name -c {online|standby}]
                [-q]
              | -display [-h logical-host-name] }
```

The command arguments are in no particular order.

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In Linux:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-f` s*etup-information-file-name*

Specifies the directory where Intelligent Integrated Management Database is installed and setup information file for the IM database that describes Port number. Depending on the configuration of Intelligent Integrated Management Database, specify the following File:

When building in a physical host environment

Intelligent Integrated Management Database Setup Information File Name

When building in a cluster environment

Cluster Environment Intelligent Integrated Management Database Setup Information File Name

The file name is specified in the form of a full path or a path relative to where this command is run. If the path contains spaces, enclose it in `""`.

`-h` *logical-host-name*

If the cluster environment Intelligent Integrated Management database setup information file name is specified on the `-f` option, a logical host name is required. For the logical host name, specify the logical host name set in JP1/Base exactly, including uppercase and lowercase letters.

Sets up the Intelligent Integrated Management database for the specified logical host. If you are not using a cluster system, you do not need to specify it.

Note that `JP1_DEFAULT` cannot be specified for the logical host name.

`-c {online|standby}`

When the `-h` option is specified, the setup type of the execution system and the standby system of the cluster configuration is specified as required. The following are the setup types that you can specify:

- `online`
  Specify to set up an execution system.
- `standby`
  Specify to set up a standby system.
  Only install Intelligent Integrated Management Database and skip building databases.

If standby is specified on the `-c` option on both the execution system and the standby system, the database will not be built. In this case, unset after the command ends, and then rerun the command.

Also, when operating a logical host in a non-clustered environment, specify online.

`-q`

Specifies that the command is to be executed without user confirmation.

`-display`

Specify if you want to check if Intelligent Integrated Management Database and Trend Data Management Services are built.

If it is already built, the following setup setting information is output as a KNAN12094-I message.

- Port number of the intelligent integrated management database
- Trend Data Management Service port number
- Data storage directory
- Installation directory
- Data retention period

Return values

0	Normal termination
1	Abnormal termination
2	Abnormal termination (If you suspect that a file or process may remain)
3	Canceled by user (if you enter `N/n` in KNAN12009-Q Message and Stopped the operation)

Log output

This command outputs the following trace log for each process: The integrated trace log is not output.

- File name
  `jimgndbsetup{1|2}.log`#
  #: `{1|2}` is a number of faces of the file.
- File size (number of faces)
  256KB (2 faces)
- Output destination
  - In Windows:
    - Physical host and Logical host

Manager-path`\log\imgndb\`

- In Linux:

- Physical host and Logical host
  `/var/opt/jp1imm/log/imgndb/`

Notes

- The contents of the executable and standby cluster environment intelligent integrated management database setup information files must be the same. When setting up the standby system, copy and use the cluster environment intelligent integrated management database setup information file used in the execution system. If the contents of the file specified in the execution system and the standby system are different, after unsetting on the standby system, copy the cluster environment intelligent integrated management database setup information file from the execution system and reexecute the command.
- When executing a command with the `-c` option, do not switch servers during execution. If you switch servers while running, unset them up after the command ends, and then rerun the command.
- The following are precautions when processing is aborted by pressing **Ctrl** + **C** or **Ctrl** + Break during command execution.

  - Ensure that the pg_ctl, postgres, and promscale processes are not running, run the `jimgndbunsetup` command, and rerun the command. If these processes are running, wait some time for them to end and rerun this command.

  - Processing is aborted, but messages may be output corrupted.

  - If you want to execute the command again after stopping the process, check the directory specified in the entry "`IMGNDBDIR`" of the Intelligent Integrated Management Database Setup Information File or the entry "`SHAREGNDBDIR`" of the Cluster Environment Intelligent Integrated Management Database Setup Information File, and if the file or directory exists, Remove them and empty them before running.
- This command cannot be multiplexed. It cannot be run concurrently with other operational commands in the Intelligent Integrated Administration database.

  For details about Intelligent Integrated Management Database operation command multiplexing execute, see *About multiple execution of the commands related to the Intelligent Integrated Management Database*.
- If you change the logical host settings with this command, the service remains stopped without restarting. In this case, you must manually start the service after running the command.
- Since the Intelligent Integrated Management Database communicates with localhost, the IP address of localhost must be resolvable. Otherwise, setup fails.

Example 1

- In case of successful completion

```
>jimgndbsetup -f intelligent-integrated-management-database-setup-informat
ion-file-name
KNAN12005-I The Intelligent Integrated Management Database will be set up.
KNAN12088-I Intelligent Integrated Management Database installation direct
ory : directory-name
KNAN12006-I Data storage directory for the Intelligent Integrated Manageme
nt Database : directory-name
KNAN12007-I Port number for the Intelligent Integrated Management Databas
e : port-number
KNAN12008-I Data retention period for the Trend Data Management Database
: data-saved-period
KNAN12009-Q Do you want to continue processing? (Y/N) :Y
KNAN12010-I Setup for the Intelligent Integrated Management Database will
now start.
```

```
KNAN12020-I Please wait.
KNAN12089-I The Intelligent Integrated Management Database will be install
ed.
KNAN12090-I The Intelligent Integrated Management Database has been instal
led.
KNAN12013-I The Intelligent Integrated Management Database will be configu
red.
KNAN12014-I The Intelligent Integrated Management Database was configured.
KNAN12012-I Setup for the Intelligent Integrated Management Database ende
d normally.
```

- In case of an abend (when the required fields in the Intelligent Integrated Management database setup information file are not specified)

```
>jimgndbsetup -f intelligent-integrated-management-database-setup-informat
ion-file-name
KNAN12005-I The Intelligent Integrated Management Database will be set up.
KNAN12022-E One or more required items are not specified in the database s
etup information file. (item name : item-name)
```

Example 2

- If you want to check the configured information

```
>jimgndbsetup -display
KNAN12094-I The Intelligent Integrated Management Database is already set
up.
Port number for the Intelligent Integrated Management Database : port-numb
er
Port number for the trend data management service : port-number
Data storage directory : directory-path
Installation directory : directory-path
Trend data retention period : retention-period
```

Example 3

- If you want to change the settings

```
>jimgndbsetup -f intelligent-integrated-management-database-setup-informat
ion-file-name
KNAN12005-I The Intelligent Integrated Management Database will be set up.
KNAN12088-I Intelligent Integrated Management Database installation direct
ory : /var/opt/jp1imm/dbms
KNAN12006-I Data storage directory for the Intelligent Integrated Manageme
nt Database : /var/opt/jp1imm/database
KNAN12007-I Port number for the Intelligent Integrated Management Databas
e : 20705
KNAN12008-I Data retention period for the Trend Data Management Database
: 64
KNAN12015-I The settings of the Intelligent Integrated Management Databas
e will be changed.
The Integrated Management Database will restart after the settings are cha
nged.
KNAN12009-Q Do you want to continue processing? (Y/N) : Y
KNAN12020-I Please wait.
KNAN12016-I The settings of the Intelligent Integrated Management Databas
e were changed.
```

jimgndbstatus

Function

This command checks the operating Status, such as starting and stopping Intelligent Integrated Management Database service and the trend data management service.

If the `-ri` option is specified, you can check the retention period of the Intelligent Integrated Management Database (Trend Data Management DB).

When the `-rs` option is specified, you can check the last execution date, end date, and next scheduled execution date for the process of deleting data that has exceeded the retention period of the Intelligent Integrated Management Database (Trend Data Management DB).

Format

```
jimgndbstatus  [{-ri | -rs}]
               [-h logical-host-name]
```

The command arguments are in no particular order.

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In Linux:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-ri`

When this option is specified, the retention period of trend data in the trend data management DB is output as the KNAN12099-I message.

`-rs`

When this option is specified, the trend data in the trend data management DB checks whether the retention period has expired and outputs the following information about the execution schedule of the deletion process of the data that has exceeded the retention period in the KNAN12054-I message.

- Last start date and time (start date and time of last run)
- Last end date and time (end date and time of last run)
- Next start date and time (next execution start date and time)

For details about the `KNAN12054-I` message, including the formats for Date/time files (Last Date/time, Last Date/time, Next Start Date/time), see the *JP1/Integrated Management 3 - Manager Messages*.

`-h` *logical-host-name*

When operating on a clustered system, specify the logical host name of the host on which the command is executed.

Checks the operating Status of Intelligent Integrated Management Database corresponding to the specified Logical host. If you are not using a cluster system, you do not need to specify it.

If this option is omitted, the logical host name specified in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not specified, the physical host name is assumed.

Note that `JP1_DEFAULT` cannot be specified for the logical host name.

Return values

0	• If neither the `-ri` option nor the `-rs` option is specified Intelligent Integrated Management Database and Trend Data Management Service are up and running. • When either the `-ri` option or the `-rs` option is specified Successful completion
1	Abnormal termination
12	Intelligent Integrated Management Database and Trend Data Management Service are stopped.
16	The Intelligent Integrated Management Database is up and the Trend Data Management Service is stopped.
17	The Intelligent Integrated Management Database is stopped, and the Trend Data Management Service is started.
20	Intelligent Integrated Management database not set up

Log output

This command outputs the following trace log for each process: The integrated trace log is not output.

- File name

  `jimgndbstatus{1|2|3|4|5|6|7|8|9|10}.log`#

  #: `{1|2|3|4|5|6|7|8|9|10}` is a number of faces of the file.

- File size (number of faces)

  5,120KB (10 faces)

- Output destination

  - In Windows:

    - Physical host

      Manager-path`\log\imgndb\`#

    - Logical host

      user-specified-path-when-created-logical-host-of-JP1/IM - Manager`\log\imgndb\`

  - In Linux:

    - Physical host

      `/var/opt/jp1imm/log/imgndb/`#

    - Logical host

      user-specified-path-when-created-logical-host-of-JP1/IM - Manager`/jp1imm/log/imgndb/`

  #

  Even in the operation of a logical host, a portion of the log is output to the physical host.

Notes

- For details about Intelligent Integrated Management Database operation command multiplexing execute, see *About multiple execution of the commands related to the Intelligent Integrated Management Database*.
- If "`unknown`" is displayed in the date and time information when the command is executed with the `-rs` option, it is possible that automatic deletion of trend data is in progress. In this case, you can wait a few moments and run the command again to obtain information about the execution schedule.

Example 1

- If neither the `-ri` option nor the `-rs` option is specified and the result is successful.

```
>jimgndbstatus
KNAN12044-I The processing to confirm the service operating status will no
w start.
KNAN12047-I The Intelligent Integrated Management Database Service is runn
ing.
KNAN12048-I The trend data management service is running.
KNAN12045-I The processing to confirm the service operating status ended n
ormally.
```

Example 2

- If the `-ri` option is specified and the end is successful.

```
>jimgndbstatus -ri
KNAN12044-I The processing to confirm the service operating status will no
w start.
KNAN12099-I The retention period is as follows:
32 days
KNAN12045-I The processing to confirm the service operating status ended n
ormally.
```

Example 3

- If the `-rs` option is specified and the end is successful.

```
>jimgndbstatus -rs
KNAN12044-I The processing to confirm the service operating status will no
w start.
KNAN12054-I The previous and next execution schedules are as follows.
Previous start date and time : [2021-07-15 17:31:06.83+09]
Previous end date and time : [2021-07-15 17:31:07.08+09]
Next start date and time : [2021-07-15 18:01:07.08+09]
KNAN12045-I The processing to confirm the service operating status ended n
ormally.
```

jimgndbstop

Function

This command stops Intelligent Integrated Management Database and Trend Data Management service.

To force the Intelligent Integrated Management database to stop, use this command with the `-f` option.

The waiting time for stopping the trend data management service is up to 10 seconds#.

#

The waiting time for a typical outage process is up to 5 seconds. If the `-f` option is specified, a maximum of 5 seconds is added to the waiting time for forced stop processing.

Also, if you are using setup to automatically start and terminate JP1/IM - Manager, use the `jco_stop` command to stop Intelligent Integrated Management Database and Trend Data Management Service. For details about the `jco_stop` command, see *jco_stop (UNIX only)*.

Format

```
jimgndbstop  -sys
             [-h logical-host-name]
             [-f]
```

The command arguments are in no particular order.

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In Linux:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-sys`

Required when this command is run. This is an option to prevent unintentional service outages.

`-h` *logical-host-name*

When operating on a clustered system, specify the logical host name of the host on which the command is executed.

Stops the Intelligent Integrated Management Database (service) and the Trend Data Management service corresponding to the specified logical host. If you are not using a cluster system, you do not need to specify it.

If this option is omitted, the logical host name specified in the environment variable `JP1_HOSTNAME` is assumed. If the environment variable `JP1_HOSTNAME` is not specified, the physical host name is assumed.

Note that `JP1_DEFAULT` cannot be specified for the logical host name.

`-f`

Specifies that Intelligent Integrated Management Database is to be forcibly stopped.

Return values

0	Normal termination
1	Abnormal termination
20	Intelligent Integrated Management database not set up

Log output

This command outputs the following trace log for each process: The integrated trace log is not output.

- File name

  `jimgndbstop{1|2|3|4|5|6|7|8|9|10}.log`#

  #: `{1|2|3|4|5|6|7|8|9|10}` is a number of faces of the file.

- File size (number of faces)

  5,120KB (10 faces)

- Output destination

  \- In Windows:

  - Physical host

    Manager-path`\log\imgndb\`#

  - Logical host

    user-specified-path-when-created-logical-host-of-JP1/IM - Manager`\log\imgndb\`

  \- In Linux:

  - Physical host

    `/var/opt/jp1imm/log/imgndb/`#

  - Logical host

    user-specified-path-when-created-logical-host-of-JP1/IM - Manager`/jp1imm/log/imgndb/`

  #

  Even in the operation of a logical host, a portion of the log is output to the physical host.

Notes

- This command cannot be multiplexed. It cannot be run concurrently with other operational commands in the Intelligent Integrated Administration database.

  For details about Intelligent Integrated Management Database operation command multiplexing execute, see *About multiple execution of the commands related to the Intelligent Integrated Management Database*.

- If you run this command and fail to stop the Intelligent Integrated Management Database and the Trend Data Management Service:

  Check the error message printed to the console, remove the cause of the error, and stop again with this command.

  If it still does not stop, stop the process using the OS function.

  For details about the process to be stopped, see *JP1/IM - Manager process (Linux)* in *Appendix B. Process List* of the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Example

- In case of successful completion

```
> jimgndbstop -sys
KNAN12064-I The trend data management service will now stop.
KNAN12068-I The trend data management service stopped.
KNAN12066-I The trend data management service stopped normally.
KNAN12063-I The Intelligent Integrated Management Database Service will no
w stop.
KNAN12067-I The Intelligent Integrated Management Database Service stoppe
d.
KNAN12065-I The Intelligent Integrated Management Database Service stoppe
d normally.
```

- In case of abend (when the database is not set up)

```
> jimgndbstop -sys
KNAN12063-I The Intelligent Integrated Management Database Service will no
w stop.
KNAN12041-E The Intelligent Integrated Management Database is not configur
ed.
```

jimgndbunsetup

Function

This command uninstalls Intelligent Integrated Management Database and Trend Data Management Service (uninstall and delete the database).

Execute this command before stopping the use of Intelligent Integrated Management Database or re-creating Intelligent Integrated Management Database. If you want to uninstall both Physical host and Logical host, you must Execute them on each host.

Format

```
jimgndbunsetup  [-h logical-host-name -c {online|standby}]
                [-q]
```

The command arguments are in no particular order.

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\imgndb\`

In Linux:

`/opt/jp1imm/bin/imgndb/`

Arguments

`-h` *logical-host-name*

When operating on a clustered system, specify the logical host name of the host on which the command is executed. For the logical host name, specify the logical host name set in JP1/Base exactly, including uppercase and lowercase letters.

Intelligent Integrated Management Database corresponding to the specified Logical host will be uninstalled. If you are not using a cluster system, you do not need to specify it.

Note that `JP1_DEFAULT` cannot be specified for the logical host name.

`-c {online|standby}`

Specify the setup type of the execution system and standby system of the cluster configuration as required. The following are the setup types that you can specify:

- `online`

  Specify to set up an execution system.

- `standby`

  Specify to set up a standby system.

  Only uninstall Intelligent Integrated Management Database and skip delete of the database.

If you specify `standby` for `-c` option on both execute system and the standby system, delete of the database is not performed. In such cases, you must manually delete the database. You can check delete targets in `KNAN12108-I` Message.

Also, when operating a logical host in a non-clustered environment, specify `online`.

`-q`

Specifies that the command is to be executed without user confirmation.

Return values

0	Normal termination
1	Abnormal termination
3	Canceled by user (if you enter `N/n` in KNAN12009-Q Message and Stopped the operation)
20	Intelligent Integrated Management database not set up

Log output

This command outputs the following trace log for each process: The integrated trace log is not output.

- File name

  `jimgndbunsetup{1|2}.log`#

  #: `{1|2}` is a number of faces of the file.
- File size (number of faces)

  256KB (2 faces)
- Output destination

  \- In Windows:

  - Physical host and Logical host

    Manager-path`\log\imgndb\`

  \- In Linux:

  - Physical host and Logical host

    `/var/opt/jp1imm/log/imgndb/`

Notes

- When executing a command with the `-c` option, do not switch servers during execution. If you switch servers while running, unset them up after the command ends, and then rerun the command.
- The following are precautions when processing is aborted by pressing **Ctrl** + **C** or **Ctrl** + **Break** during command execution.

  \- Ensure that the pg_ctl, postgres, and promscale processes are not running, run the `jimgndbunsetup` command, and rerun the command. If these processes are running, wait some time for them to end and rerun this command.

  \- Processing is aborted, but messages may be output corrupted.
- This command cannot be multiplexed. It cannot be run concurrently with other operational commands in the Intelligent Integrated Administration database.

  For details about Intelligent Integrated Management Database operation command multiplexing execute, see *About multiple execution of the commands related to the Intelligent Integrated Management Database*.
- If a `KNAN12105-E` or `KNAN12107-E` error message is output, or if a `KNAN12108-I` message is output due to an error, check the directory name in the message and manually delete the data in the corresponding directory.

Example

- In case of successful completion

```
>jimgndbunsetup
KNAN12035-I Unsetup of the Intelligent Integrated Management Database wil
l be performed.
KNAN12009-Q Do you want to continue processing? (Y/N) :Y
KNAN12036-I Unsetup of the Intelligent Integrated Management Database wil
l now start.
KNAN12020-I Please wait.
KNAN12104-I The Intelligent Integrated Management Database was uninstalle
d.
KNAN12106-I The data storage directory of the Intelligent Integrated Manag
ement Database was deleted.
KNAN12038-I Unsetup of the Intelligent Integrated Management Database ende
d normally.
```

- In case of abend (when the database is not set up)

```
>jimgndbunsetup
KNAN12035-I Unsetup of the Intelligent Integrated Management Database wil
l be performed.
KNAN12041-E The Intelligent Integrated Management Database is not configur
ed.
```

jimmail (Windows only)

Function

This command sends an email to a specified email address.

To use the `jimmail` command to send an email, you must set the email environment definition file.

You can execute this command independently regardless of whether the JP1/IM - Manager service is running. The following table describes the functions of JP1/IM - Manager that can be used to send an email.

Table 1–48: JP1/IM - Manager functions used to send an email by using the jimmail command

Function	Description
Automated action	An email can be sent by automated action.
Monitoring action and delay statuses	An email can be sent by using the notification command when an action error is detected.
Health check	An email can be sent by using the notification command when a JP1/IM - Manager process error is detected.
Command execution (Command button)	An email can be sent by pressing a command button.

If the maximum length of a command line is exceeded, redefine the email contents so that the command line of the `jimmail` command can fit within the limit.

Format

```
jimmail [-to destination-email-address[,destination-email-address...]]
        [-s email-subject]
        [-b email-text]
        [-rh logical-host-name]
```

Execution permission

Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console.)

Storage directory

Console-path`\bin\`

Arguments

`-to` *destination-email-address*`[,`*destination-email-address*`...]`

This option specifies the email destination address.

A maximum of 20 email addresses can be specified. Note, however, that addresses exceeding the maximum command line length cannot be specified. When specifying multiple email addresses, use a comma (`,`) as a separator. Any one-byte space or tab between an email address and a comma is ignored. Consecutive commas (`,`) are treated as a single comma, and commas at the beginning and at the end are ignored. If the same email address is specified more than once, the email message is sent to the specified address only once.

If the number of specified email addresses exceeds the maximum limit, the `KAVB8725-E` message is output, and the operation terminates abnormally.

You can specify 1 to 256 bytes of characters for the destination email address. One-byte alphanumeric characters, at marks (`@`), hyphens (-), underscores (_), and periods (`.`) can be specified.

This option can be omitted. If you omit this option, processing continues using the email address specified for the `DefaultTo` parameter (default destination email address) in the email environment definition file as the destination. When an email is being processed, the message sent to the email address of the `DefaultTo` parameter is not output.

If the `-to` option is omitted, and no email address is specified for the `DefaultTo` parameter, the `jimmail` command outputs an error message, and the operation terminates abnormally.

If both the `-to` option and the `DefaultTo` parameter are set, the `-to` option takes precedence.

The `jimmail` command does not check if the specified email address is valid.

`-s` *email-subject*

This option specifies the email subject.

You can specify 1 to 512 bytes of characters. The character count is determined by calculating the byte count based on the email character encoding specified by the `Charset` parameter in the email environment definition file. When event or action information is to be inherited, the maximum-length check is performed by calculating the length after `$`*variable-name* has been replaced. If the calculated length exceeds the maximum length, the value specified for the `MailSubjectCutting` parameter in the email environment definition file determines whether the subject is to be cut to allow the email to be sent.

- When the `MailSubjectCutting` parameter value is `OFF`, the `KAVB8708-E` message is output, and the command terminates abnormally.
- When the `MailSubjectCutting` parameter value is `ON`, characters for the email subject exceeding 512 bytes are discarded according to the character encoding specified for the `Charset` parameter, and the email is sent. When an email subject exceeds 512 bytes, characters exceeding 512 bytes are discarded. If an email is sent after the exceeding characters in the subject are discarded, the `KAVB8724-W` message appears before the `KAVB8729-I` message (indicating the email is sent successfully).

This option can be omitted. If you omit this option, the subject of the email will be a null character (`""`).

If the email subject contains blank characters, enclose the subject in double-quotation marks (`"`).

Even if you specify `\n`, a line break is not created in the email subject. If you specify `\n`, it appears as is. Line feed codes and control characters are converted into one-byte spaces.

`-b` *email-text*

This option specifies the email text.

You can specify 1 to 4,096 byte characters for the email text. The number of characters is checked by the number of bytes, according to the character encoding of the email specified by the `Charset` parameter in the email environment definition file. To inherit event or action information, check the maximum length after replacing `$`*variable-name*.

You can specify 1 to 512 byte characters including linefeed codes for a line. If the characters exceed 512 bytes, insert a linefeed code so that the line will be a maximum of 512 bytes including linefeed codes. When a line exceeds the number, no warning message is output.

This option can be omitted. If you omit this option, the email text will be null characters (`""`).

If there is no linefeed code at the end of the last line, a linefeed code is inserted.

If the email text contains null characters, enclose and specify the email text by the double-quotation marks (`"`).

When `\n` is specified in the email text, a new line starts after the linefeed code specified by the `MailNewLine` parameter in the email environment definition file. If the value of the parameter is not `CRLF`, `CR`, or `LF`, `\n` is converted to a single-byte space.

To enter `\n` as a character string, specify it as `\\n`.

`-rh` *logical-host-name*

When JP1/IM - Manager is used in a cluster, the `-rh` option specifies the email environment definition file to use. With this option, specify if the `jimmail` command uses the email environment definition file on a physical host, or in the shared folder on a logical host.

If you specify this option, the email environment definition file is loaded to a shared folder on the specified logical host, and the email is sent.

If you omit this option, the email environment definition file is loaded to a physical host, and then the email is sent.

Note that if you omit this option, the logical hostname specified for the `JP1_HOSTNAME` environment variable is assumed. If he `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you do not use JP1/IM - Manager in a cluster, it is not necessary to specify this option.

Note

- Specify the subject and text of the email specified in the command line within the range of character encoding defined in the email environment definition file. For details about the email environment definition file, see *Email environment definition file (jimmail.conf)* in *Chapter 2. Definition Files*.
- The following control characters included in the event information passed to an email sent by the `jimmail` command (executed as an automated action or by clicking a command button) are converted to a single-byte space (0x20):

  0x01 to 0x1F excluding 0x09 (tab), and 0x7F

  For example, if the message obtained by `$EVMSG` includes 0x0A (line feed code), 0x0A is converted to 0x20 (single-byte space).

Return values

Return value	Description
`0`	Normal termination
`1`	Argument error
`2`	Destination email address is not specified.
`3`	Error while reading the email environment definition file
`4`	Format error of the email environment definition file (Invalid setting value, essential item not specified, invalid parameter)
`5`	A timeout error occurred while connecting to the SMTP server
`6`	SMTP server rejected the login
`7`	Connection to the SMTP server could not be established
`8`	A timeout error occurred while connecting to the POP3 server
`9`	POP3 server rejected the login
`10`	`Connection to the POP3 server could not be established`
`11`	Sending an email failed
`12`	Insufficient memory
`13`	Execution permission error
`255`	Other errors

Example

The following is an email notification example from the manager host (`jp1imhost001`) to the system administrator (`user@hitachi.com`) about a failure on the monitored host (`gyoumu001`) through automated action, and the contents of the email to be sent:

```
jimmail.exe -to user@hitachi.com -s "[severity:$EVSEV] Failure notification
" -b "A failure occurred on the business server. \n---\n event DB serial num
ber=$EVSEQNO\nevent-occurrence-date-and-time=$EVDATE $EVTIME\nEvent ID=$EVID
BASE\nSeverity=$EVSEV\nProduct name=$EV"PRODUCT_NAME"\nMessage=$EVMSG\n---\n
From:IM-M host ($ACTHOST)"
```

Example of email notification:

Source (From)	`admin@hitachi.com`
Destination (To)	`user@hitachi.com`
Email subject	`[Severity:Error] Failure notification`

Email text	`A failure occurred on the business server.`
	`---`
	`Serial number in the event database=1234567`
	`Event occurrence date and time=2014/01/01 10:00:00`
	`Event ID=000A`
	`Severity=Error`
	`Product name=/HITACHI/XXXXX/JP1`
	`Message=A system error occurred on the business server`
	`---`
	`From:IM-M host (jp1imhost001)`

jimmailpasswd (Windows only)

Function

Sets the POP before SMTP or SMTP-AUTH authentication password in the email environment definition file. This command can be executed independently regardless of the running status of the JP1/IM - Manager service.

Before executing this command, set the following items in the email environment definition file:

- Specify `POP` or `SMTP` for the `AuthMethod` parameter.
- Specify the authentication account name for the `AuthUser` parameter.

If you execute this command without specifying these parameters, the `KAVB8714-E` or `KAVB8736-E` message is output, and the operation terminates abnormally.

Format

```
jimmailpasswd {-p new-authentication-password | -d}
              [-rh logical-host-name]
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console).

Storage directory

Console-path`\bin\`

Arguments

`-p` *new-authentication-password*

This option sets the authentication password when POP before SMTP or SMTP-AUTH authentication is used to connect to an email server in the email environment definition file.

Specify an authentication password from 1 to 127 bytes for the argument of the option. The authentication password of the argument cannot be omitted.

Permitted characters are one-byte characters other than control characters (`0x00` to `0x1F`, and `0x7F` to `0x9F`). Multi-byte characters cannot be specified. The password is case sensitive.

If you omit a password for the argument of the option, the `KAVB8704-E` message is output, and the operation terminates abnormally.

`-d`

This option deletes an authentication password from the email environment definition file. If you execute this command with this option specified, the setting value for the `AuthPassword` parameter (password section) in the email environment definition file is deleted.

The `-d` option cannot be specified with the `-p` option.

`-rh` *logical-host-name*

When JP1/IM - Manager is used in a cluster, the `-rh` option specifies the email environment definition file to use. With this option, specify if the `jimmail` command uses the email environment definition file on a physical host, or in the shared folder on a logical host.

When you specify this option, an authentication password is set in the email environment definition file in a shared folder on the specified logical host.

If you omit this option, an authentication password is set in the email environment definition file on a physical host.

Note that if you omit its option, the logical host name specified for the `JP1_HOSTNAME` environment variable is assumed. If the `JP1_HOSTNAME` environment variable is not specified, the physical host name is assumed. If you do not use JP1/IM - Manager in a cluster, you do not need to specify this option.

Example 1

Specify the authentication password `ABCD` in the email environment definition file:

```
$ jimmailpasswd -p ABCD
KAVB8731-I Command (jimmailpasswd) started.
KAVB8730-I Password was set successfully.
KAVB8732-I Command (jimmailpasswd) ended normally.
```

Example 2

Set the authentication password `ABCD` in the email environment definition file on the logical host (`ronri`):

```
$ jimmailpasswd -p ABCD -rh ronri
KAVB8731-I Command (jimmailpasswd) stated.
KAVB8730-I Password was set successfully.
KAVB8732-I Command (jimmailpasswd) ended normally.
```

Example 3

Delete the authentication password from the email environment definition file:

```
$ jimmailpasswd -d
KAVB8731-I Command (jimmailpasswd) started.
KAVB8734-I Password was deleted successfully.
KAVB8732-I Command (jimmailpasswd) ended normally.
```

jimnodecount

Function

This command counts the number of nodes managed by JP1/IM - Manager. This command also outputs a file that contains a list of managed nodes.

This command can be executed regardless of whether JP1/IM - Manager is running.

The nodes that this command can count (as nodes managed by JP1/IM - Manager) are JP1/Base on the host defined in the configuration definition information and remotely monitored hosts.

Note that JP1/Base installed on a host that is not defined in the configuration definition information is not counted as a managed node. JP1/Base on such a host must be counted by the user manually.

Format

```
jimnodecount[ -h logical-host-name | -m]
            [ -o output-file-name]
```

Execution permission

In Windows: Administrator permissions

In UNIX: Superuser permissions

Storage directory

In Windows:

Manager-path`\bin\`

In UNIX:

`/opt/jp1imm/bin/`

Arguments

`-h` *logical-host-name*

If JP1/IM - Manager is operating in a cluster system, use this option to specify which type of host (physical or logical) the nodes to be counted by the `jimnodecount` command are managed by.

If the `-h` option is specified, the command counts the nodes managed by the specified logical host.

If the `-h` option is not specified, the command counts the nodes managed by the logical host specified in the `JP1_HOSTNAME` environment variable. If no logical host name is specified in that environment variable, the command counts the nodes managed by the physical node.

If JP1/IM - Manager is not operating in a cluster system, you do not need to specify this option.

`-m`

If JP1/IM - Manager is operating in a cluster system, use this option to specify whether the `jimnodecount` command counts the total number of nodes managed by the physical host and logical host.

If the `-m` option is specified, the command counts the number of all managed nodes.

If the `-m` option is not specified, the command counts the number of nodes managed by the logical host specified in the `JP1_HOSTNAME` environment variable. If no logical host name is specified in that environment variable, the command counts the number of nodes managed by the physical host.

`-o` *output-file-name*

This option specifies the managed-node list file to which a list of managed nodes is to be output. If the specified file already exists, the contents of the existing file are overwritten.

The output file name can be specified as a relative path or absolute path. If a relative path is used to specify the output file name, the directory where the `jimnodecount` command is executed is used as the base of the relative path. If you specify a file whose name begins with a hyphen (`-`), to distinguish the file name from an option name, use a relative path that begins with the current directory (for example, `./-foo`) or an absolute path. Note that the length of the file name you specify must not exceed 250 bytes including the length of the path.

Network paths cannot be specified as the output file name.

Also note that in Windows, the file name you specify must not include the following character strings:

- Colon (`:`), question mark (`?`), double quotation mark (`"`), left angle bracket (<), right angle bracket (>), and vertical bar(`|`)
- A string that completely matches one of the following strings (ignoring case): `CON`, `PRN`, `AUX`, `NUL`, `COM1`, `COM2`, `COM3`, `COM4`, `COM5`, `COM6`, `COM7`, `COM8`, `COM9`, `LPT1`, `LPT2`, `LPT3`, `LPT4`, `LPT5`, `LPT6`, `LPT7`, `LPT8`, or `LPT9`

Output format

When you execute the `jimnodecount` command, the number of managed nodes is output in the format below.

Note that if an error occurs during execution of the command, the number of managed nodes is not output.

```
number-of-managed-nodes
```

Note

In a cluster system configuration in which JP1/IM - Managers on multiple logical hosts manage the same host as a managed node, each logical host is counted as a single host by the `jimnodecount -m` command. In this case, reduce the number of managed nodes appropriately:

Return values

0	Normal termination
43	The `jimnodecount` command was executed while the remote configurations were being applied or the `jcfimport` command was being executed.
84	Argument error
85	Execution permission error
127	Other error

Format of the managed-node list file

The following describes the format of the managed-node list file. The numbers at the beginning of each line (1 to 12) indicate line numbers, which are not output in the actual file.

```
 1  output-time
 2  The number of managed nodes : number-of-managed-nodes
 3  M  /manager-host-name
 4  B  /manager-host-name/host-name-for-JP1/Base-on-host-defined-in-configur
ation-definition-information
 5  R  /manager-host-name/name-of-remotely-monitored-host
 6  BR /manager-host-name/host-name-for-JP1/Base-on-remotely-monitored-host-
defined-in-configuration-definition-information
 7  B  /manager-host-name/site-manager-host-name
 8  B  /manager-host-name/site-manager-host-name/host-name-for-JP1/Base-on-h
ost-defined-in-configuration-definition-information
 9  R  /manager-host-name/site-manager-host-name/name-of-remotely-monitored-
host
10  BR /manager-host-name/site-manager-host-name/host-name-for-JP1/Base-on-r
emotely-monitored-host-defined-in-configuration-definition-information
11  B  /manager-host-name/relay-manager-host-name
12  B  /manager-host-name/relay-manager-host-name/host-name-for-JP1/Base-on-
host-defined-in-configuration-definition-information
```

Lines 2 to 12 are the managed-node block, which consists of the number of managed nodes on line 2 and the managed-node list on lines 3 to 12.

Description of the elements output to the managed-node list file

output-time

The time that the `jimnodecount` command was executed and the managed-node list file was output is indicated here.

```
YYYY/MM/DD hh:mm:ss
```

(*YYYY*: year, *MM*: month, *DD*: day, *hh*: hour, *mm*: minute, *ss*: second)

Managed-node block

The elements of a managed-node block are as follows:

- `The number of managed nodes :` *number-of-managed-nodes*

  The number of managed nodes counted by the command is indicated here.

- Managed-node list

  type-of-managed-node`/`*host-name*`[/`*host-name...*`]`

  The strings output for *type-of-managed-node* are described below.

Type	Description
`M∆ ∆`	Manager host on which the `jimnodecount` command was executed
`B∆ ∆`	JP1/Base on a host that is defined in the configuration definition information and is not the Manager host on which the `jimnodecount` command was executed
`R∆ ∆`	Remotely monitored host
`B∆`	JP1/Base on a remotely monitored host that is defined in the configuration definition information

Legend: ∆: A single-byte space

The managed-node block output format differs depending on whether the `-m` option is specified.

If the `-m` option is not specified:

Only one managed-node block is output.

The following shows an example of the file output if the `-m` option is not specified.

Integrated manager	Site manager	Agent
Physical host (`kanri`)	`tokyo`	`jp1ag1`
	`osaka`	`rhost1`

Integrated manager	Site manager	Agent
		jp1ag2

```
2016/04/28 09:00:00
The number of managed nodes : 6
M  /admin
B  /admin/tokyo
B  /admin/tokyo/jp1ag1
B  /admin/osaka
R  /admin/osaka/rhost1
BR /admin/osaka/jp1ag2
```

If the `-m` option is specified:

Multiple managed-node blocks are output. The managed-node block for the physical host is output before the managed-node blocks for logical hosts. The managed-node blocks for logical hosts are output in the ascending order of logical host names.

The following shows an example of the file output if the `-m` option is specified.

Integrated manager	Site manager	Agent
Physical host (`admin`)	`tokyo`	`jp1ag1`
Logical host (`adminL1`)	`osakaA`	`jp1ag2`
	`osakaB`	`jp1ag3`
Logical host (`adminL2`)	`nagoyaA`	`jp1ag4`
Logical host (`adminL3`)	`nagoyaB`	`jp1ag5`

```
2016/11/26 09:00:00
The number of managed nodes : 3
M  /admin
B  /admin/tokyo
B  /admin/tokyo/jp1ag1
The number of managed nodes : 5
M  /adminL1
B  /adminL1/osakaA
B  /adminL1/osakaA/jp1ag2
B  /adminL1/osakaB
B  /adminL1/osakaB/jp1ag3
KAVB8201-E-or-KAVB8202-E-message-text#
The number of managed nodes : 3
M  /adminL3
B  /adminL3/nagoyaB
B  /adminL3/nagoyaB/jp1ag5
```

#: Because the command failed to count the number of nodes managed by logical host `adminL2`, a message (KAVB8201-E or KAVB8202-E) was output. For details about the message, see the *JP1/Integrated Management 3 - Manager Messages*.

jp1cc_setup (UNIX only)

Function

This command sets up an operating environment for JP1/IM - Manager (Central Console).

Use this command only after you have uninstalled JP1/Base on a computer where both JP1/IM - Manager and JP1/Base were installed and you have then re-installed JP1/Base. When you use Hitachi Program Product Installer to perform a new installation or an overwrite installation of JP1/IM - Manager, there is no need to execute this command.

Format

```
jp1cc_setup
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1cons/bin/`

jp1cshaverup.bat (Windows only)

Function

This command upgrades a logical host environment that was set up for JP1/IM - Manager (Central Scope). Use this command after you have upgraded your JP1/IM - Manager (Central Scope) in a logical host environment.

Format

```
jp1cshaverup.bat -h logical-host-name
                 [-w work-directory]
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Scope-path`\bin\`

Note: This command is not included in JP1/IM - Manager for Linux.

Arguments

`-h` *logical-host-name*

Specifies the name of the logical host that is to be upgraded. If this option is omitted, an error results.

`-w` *work-directory*

Specifies the full path of a work folder that will be used to upgrade the logical host environment for JP1/IM - Manager (Central Scope). If the path contains a space, enclose the entire path in double-quotation marks (`"`).

If this option is omitted, *Scope-path*`\tmp\` is assumed.

Notes

- You must terminate JP1/IM - Manager before you execute this command. An error results if this command is executed while JP1/IM - Manager is running.
- Once the `jp1cshaverup.bat` command has been executed, JP1/IM - Manager (Central Scope) runs under the new version that has been installed, and you can no longer log in from the Monitoring Tree (Editing) window of JP1/IM - View version 08-01 or earlier.
- Return values

`0`	Normal termination
`1`	Specified logical host name was not found
`2`	Argument error
`4`	No permission to execute the command
`12`	Insufficient memory
`13`	Insufficient disk capacity
`31`	Database initialization error

32	Data access error
42	A service is running
45	An attempt was made to execute the command on the new version of the database
99	Other error

Examples

Upgrade the `logicalhost` logical host environment for the JP1/IM - Manager (Central Scope) instance that is running under version 08-01; use the `C:\temp\` work folder:

```
jp1cshaverup -h logicalhost -w C:\temp
```

Example output

```
The upgrade processing started.
KAVB7750-I Upgrading of the database version has finished.
KAVB7624-I The jcsdbconvert command finished successfully.
The upgrade processing ends successfully.
```

Return values

0	Normal termination
1	Abnormal termination

jp1cc_setup_cluster (UNIX only)

Function

This command sets up an operating environment for a logical host of JP1/IM - Manager (Central Console). Use this command for environment setup in a cluster system.

Set up the environment for the primary node first, and then set up the standby node.

In the environment setup for the primary node, you must specify the logical host name and shared directory name. When you execute this command, information such as definition files is copied to the specified shared directory; therefore, you must have already made the shared disk available for use.

In the environment setup for the standby node, specify only the logical host name. The operating environment is set up on the basis of the information specified for the executing node.

Before you start setting up an environment for the secondary node, you must use the `jbsgetcnf` and `jbssetcnf` commands of JP1/Base to copy to the standby node the common definition information set at the executing node.

When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

Format

```
jp1cc_setup_cluster -h logical-host-name
                    [-d shared-directory-name]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

Specifies a host name for the logical host whose environment is to be set up. The permitted length is from 1 to 63 bytes characters.

Set the specified logical host name in the `hosts` file and in the name server to enable TCP/IP communication.

`-d` *shared-directory-name*

Specifies a shared directory for storing the information that is to be inherited during node switching. Specify a directory on the shared disk. The permitted length is from 1 to 165 bytes characters.

The command creates the directories listed below in the specified shared directory and then copies definition files from `/etc/opt/jp1cons/conf/`. Appropriate permissions are set for the created directories. Do not change the set permissions of the directories.

Table 1–49: Directories created by the jp1cc_setup_cluster command

Type of files to be stored	Directory
Definition files	*shared-directory-name*/jp1cons/conf/
Log files	*shared-directory-name*/jp1cons/log/
Temporary files	*shared-directory-name*/jp1cons/tmp/
History files#	*shared-directory-name*/jp1cons/operation/

#: The processing of the correlation event generation function is output as history data.

Change the definition files, if necessary.

Notes

- You must set a logical host for each node.
- You must make the shared disk available for use before you set up an environment for the primary node by executing the jp1cc_setup_cluster command.

Return values

0	Normal termination
1	Abnormal termination

Examples

Set up an environment with the following conditions:

```
Logical host name: lnode0
Shared disk: /shdsk/lnode0
```

- Setting up the logical host environment at the primary server

```
jp1cc_setup_cluster -h lnode0 -d /shdsk/lnode0
```

- Setting up the logical host environment at the secondary server

```
jp1cc_setup_cluster -h lnode0
```

jp1cf_setup (UNIX only)

Function

This command sets up an operating environment for the IM Configuration Management process of JP1/IM - Manager.

Use this command only after you have uninstalled JP1/Base on a computer where both JP1/IM - Manager and JP1/Base were installed and you have then re-installed JP1/Base.

Format

```
jp1cf_setup
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1imm/bin/imcf`

Return values

0	Normal termination
1	Abnormal termination

jp1cf_setup_cluster (UNIX only)

Function

This command sets up an environment for IM Configuration Management when you are operating in a cluster system.

This cluster setup for IM Configuration Management applies to both the primary node and the standby node of the logical host. When the `-d` option is specified, the command sets up the primary node; when the `-d` option is omitted, the command sets up the secondary node.

The following table lists and describes the settings for the primary and secondary nodes.

Table 1–50: Settings for the primary and secondary nodes

Host where command is executed	Setting item	Overview of setting
Primary node	Common definition settings for the logical host	Use the `jbsgetcnf` and `jbssetcnf` commands to set the common definitions of IM Configuration Management for the physical host to also be the common definitions for the logical host. Some information (such as directory names) must be changed.
	Creating the shared directory	Create the required directories under the shared directory.
	Copying the definition files	Copy the definition files from `/opt/jp1imm/conf/imcf` to the directories under *shared-directory*`/jp1imm/conf/imcf`.
	Setting startup of IM Configuration Management for the instance of Central Console on the logical host	Use the `jcoimdef` command to set IM Configuration Management Service to start according to process management of the instance of Central Console on the logical host.
	Changing the communication method for IM Configuration Management on the physical host	Change the communication method for IM Configuration Management on the physical host to the IP binding method.
Secondary node	Changing the communication method on the physical host	Same as above

Setting the common definitions

Cluster setup of IM Configuration Management sets the values shown below in the common definitions for the logical host.

Table 1–51: Common definitions for the logical host

Path	Key name	Setting
logical-host-name`\JP1CONF\`	`JP1CONFIG_CONFDIR`	*shared-directory-name*`/jp1imm/conf/imcf`
	`JP1CONFIG_TMPDIR`	*shared-directory-name*`/jp1imm/tmp`
	`JP1CONFIG_LOGDIR`	*shared-directory-name*`/jp1imm/log/imcf`
	`JP1CONFIG_DATADIR`	*shared-directory-name*`/jp1imm/data/imcf`
	`JP1_BIND_ADDR`	`IP`

Creating the shared directory

Cluster setup of IM Configuration Management creates the directories shown below. Appropriate permissions are set for the created directories. Do not change the set permissions of the directories.

Table 1–52: Directories created when the jp1cf_setup_cluster command is executed

Type of files to be stored	Directory
Definition files	*shared-directory-name*/jp1imm/conf/imcf
Log files	*shared-directory-name*/jp1imm/log/imcf
Temporary files	*shared-directory-name*/jp1imm/tmp
Data for the system hierarchy and profiles	*shared-directory-name*/jp1imm/data/imcf

Setting startup of IM Configuration Management for the instance of Central Console on the logical host

Execute the `jcoimdef` command to add the IM Configuration Management startup settings to the process management of the instance of Central Console on the same logical host.

Changing the communication method for IM Configuration Management on the physical host

Cluster setup of IM Configuration Management changes the communication method for the physical host to the IP binding method by changing the value of `JP1_BIND_ADDR` under the `JP1_DEFAULT\JP1CONFIG\` common definition to `IP`.

Format

```
jp1cf_setup_cluster  -h logical-host-name
                     [-d shared-directory-name]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1imm/bin/imcf`

Arguments

`-h` *logical-host-name*

When you are operating in a cluster system, this option specifies the logical host name of the host where the command is executed. The command reorganizes the database for the specified logical host. The permitted length is from 1 to 63 bytes characters. If this option is omitted, an error results.

`-d` *shared-directory-name*

Specifies the shared directory for the logical host in order to set up the primary node. When this option is omitted, the command sets up the secondary node. The permitted length is from 1 to 165 bytes characters.

Return values

0	Normal termination
1	Abnormal termination

Notes

- When you set up the primary node, you must mount the shared disk in order to copy the definition files to the shared directory and create a monitoring object database.
- You must set up a logical host for each node.

- When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

jp1cfhasetup (Windows only)

Function

This command sets up an environment for IM Configuration Management when you are operating in a cluster system.

Before you execute this command, you must set up the logical host of JP1/Base.

When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

Format

```
jp1cfhasetup
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Manager-path`\bin\imcf\`

Notes

- If you want to execute the `jp1cfhasetup` command, execute the `jp1cohasetup` command first.
- Set a logical host for each node.
- You must have set up the logical host for JP1/Base beforehand. For details about how to set up JP1/Base, see the *JP1/Base User's Guide*.

jp1cohasetup (Windows only)

Function

This command displays the Settings for Central Console Cluster System dialog box, which is used to set up an operating environment for the logical host of JP1/IM - Manager (Central Console). Use this command to set up an environment for JP1/IM - Manager (Central Console) in a cluster system.

When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

Format

```
jp1cohasetup
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Console-path`\bin\`

Notes

- Use this command to set up an environment for JP1/IM - Manager (Central Console) in a cluster system. Use the `jp1cshasetup` command to set up an environment for JP1/IM - Manager (Central Scope).
- Set a logical host for each node.
- You must have set up the logical host for JP1/Base beforehand. For details about how to set up JP1/Base, see the *JP1/Base User's Guide*.

jp1cohaverup

Function

This command upgrades a logical host environment that was set up for JP1/IM - Manager. Use this command after you have upgraded your JP1/IM - Manager in a logical host environment.

Format

```
jp1cohaverup -h logical-host-name
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In UNIX: Superuser permissions

Storage directory

In Windows:
Console-path`\bin\`

In UNIX:
`/opt/jp1cons/bin/`

Arguments

`-h` *logical-host-name*

Specifies the name of the logical host to be upgraded. If this option is omitted, an error results.

Notes

- You must terminate JP1/IM - Manager before you execute this command. An error results if this command is executed while JP1/IM - Manager is running.
- Execute this command only on the primary host. Make sure that the shared disk is mounted when the command executes. Do not execute this command on the secondary host.
- After you have executed this command, you must back up the common definition information from the primary host, copy the backup common definition information to the secondary host, and then use the `jbssetcnf` command to set the information.
- If you have installed a corrected edition of the same version by overwriting, there is no need to execute this command.

Return values

`0`	Normal termination
`1`	Abnormal termination

Examples

Upgrade logical host `host01`:

```
jp1cohaverup -h host01
```

Example output

```
jp1cohaverup -h host01
KAVB9101-I The upgrading of the logical host environment will now start.
KAVB9102-I The upgrading of the logical host environment has finished.
```

jp1cs_setup (UNIX only)

Function

This command sets up an operating environment for JP1/IM - Manager (Central Scope).

Use this command only after you have uninstalled JP1/Base on a computer where both JP1/IM - Manager and JP1/Base were installed and you have then re-installed JP1/Base. When you use Hitachi Program Product Installer to perform a new installation or an overwrite installation of JP1/IM - Manager, there is no need to execute this command.

You must terminate JP1/IM - Manager before you use this command.

Format

```
jp1cs_setup
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1scope/bin/`

Return values

0	Normal termination
1	Abnormal termination

jp1cs_setup_cluster (UNIX only)

Function

This command sets up an operating environment for a logical host of JP1/IM - Manager (Central Scope). Use this command for environment setup in a cluster system.

Set up the environment for the primary node first, and then set up the standby node.

In the environment setup for the primary node, you must specify the logical host name and shared directory name. When you execute the command, information such as definition files is copied to the specified shared directory; therefore, you must have already made the shared disk available for use.

In the environment setup for the standby node, specify only the logical host name. The operating environment is set up based on the information specified for the executing node.

Before you start setting up an environment for the secondary node, you must use the `jbsgetcnf` and `jbssetcnf` commands of JP1/Base to copy to the standby node the common definition information set at the executing node.

Before you use this command, terminate JP1/IM - Manager.

When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

Format

```
jp1cs_setup_cluster -h logical-host-name
                    [-d shared-directory-name]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

Specifies a host name for the logical host whose environment is to be set up. The permitted length is from 1 to 63 bytes characters.

Set the specified logical host name in the `hosts` file and in the name server to enable TCP/IP communication.

`-d` *shared-directory-name*

Specifies a shared directory for storing the information that is to be inherited during node switching. Specify a directory on the shared disk. The permitted length is from 1 to 165 bytes characters.

The command creates the directories listed below in the specified shared directory and then copies definition files from `/etc/opt/jp1scope/conf/`. Appropriate permissions are set for the created directories. Do not change the set permissions of the directories.

Table 1–53: Directories created by the jp1cs_setup_cluster command

Type of files to be stored	Directory
Definition files	*shared-directory-name*`/jp1scope/conf/`
Log files	*shared-directory-name*`/jp1scope/log/`
Temporary files	*shared-directory-name*`/jp1scope/tmp/`
Database information	*shared-directory-name*`/jp1scope/database/`

Change the definition files, if necessary.

Notes

- You must set a logical host for each node.
- You must make the shared disk available for use before you set up an environment for the primary node by executing the `jp1cs_setup_cluster` command.

Return values

`0`	Normal termination
`1`	Abnormal termination

Examples

Set up an environment with the following conditions:

```
Logical host name: lnode0
Shared disk: shdsk/lnode0
```

- Setting up the logical host environment at the primary server

```
jp1cs_setup_cluster -h lnode0 -d /shdsk/lnode0
```

- Setting up the logical host environment at the secondary server

```
jp1cs_setup_cluster -h lnode0
```

jp1cshasetup (Windows only)

Function

This command displays the Settings for Central Scope Cluster System dialog box that is used to set up an operating environment for the logical host of JP1/IM - Manager (Central Scope). Use this command to set up an environment for JP1/IM - Manager (Central Scope) in a cluster system.

When you execute this command, the socket binding method used for TCP/IP communication is changed to the IP binding method. The command changes this setting for the physical host and for the logical host that is to be created. For details about the socket binding method used for TCP/IP communication, see the documentation for the applicable OS.

Format

```
jp1cshasetup
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Scope-path`\bin\`

Notes

- Use this command to set up an environment for JP1/IM - Manager (Central Scope) in a cluster system. Use the `jp1cohasetup` command to set up an environment for JP1/IM - Manager (Central Console).
- Set a logical host for each node.
- You must have set up the logical host for JP1/Base beforehand. For details about how to set up JP1/Base, see the chapter that describes setup for operation in a cluster system in the *JP1/Base User's Guide*.

  You must have already set up a logical host for JP1/IM - Manager (Central Console).

jp1cshaverup (UNIX only)

Function

This command upgrades a logical host environment that was set up for JP1/IM - Manager (Central Scope). Use this command after you have upgraded your JP1/IM - Manager (Central Scope) in a logical host environment.

Format

```
jp1cshaverup -h logical-host-name
             [-w work-directory]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1scope/bin/`

Arguments

`-h` *logical-host-name*

Specifies the name of the logical host to be upgraded. If this option is omitted, an error results.

`-w` *work-directory*

Specifies the full path of a work directory that will be used to upgrade the logical host environment for JP1/IM - Manager (Central Scope).

If this option is omitted, `/opt/jp1scope/tmp/` is assumed.

Notes

- You must terminate JP1/IM - Manager before you execute this command. An error results if this command is executed while JP1/IM - Manager is running.
- Once the `jp1cshaverup` command has been executed, JP1/IM - Manager (Central Scope) runs under the new version that has been installed, and you can no longer log in from the Monitoring Tree (Editing) window of JP1/IM - View version 08-01 or earlier.

Return values

`0`	Normal termination
`1`	Specified logical host name was not found
`2`	Argument error
`4`	No permission to execute the command
`12`	Insufficient memory
`13`	Insufficient disk capacity
`31`	Database initialization error
`32`	Data access error
`42`	A service is running

45	An attempt was made to execute the command on the new version of the database
99	Other error

Examples

Upgrade the `logicalhost` logical host environment for the JP1/IM - Manager (Central Scope) instance that is running under version 08-01; use the `/temp/` work directory:

```
jp1cshaverup -h logicalhost -w /temp
```

Example output

```
The upgrade processing started.
KAVB7750-I Upgrading of the database version has finished.
KAVB7624-I The jcsdbconvert command finished successfully.
The upgrade processing ends successfully.
```

jp1csverup (UNIX only)

Function

This command upgrades a physical host environment that has been set up for JP1/IM - Manager (Central Scope) under version 08-01 or earlier. Use this command after you have upgraded your JP1/IM - Manager (Central Scope) from version 08-01 or earlier.

You must execute this command in order to use the functions of a new version of JP1/IM - Manager (Central Scope) that has been installed. However, if you want to use only the functions supported by version 08-01 or earlier, do not execute this command.

Format

```
jp1csverup [-w work-directory]
```

Execution permission

Superuser permissions

Storage directory

`/opt/jp1scope/bin/`

Note: This command is not included in JP1/IM - Manager for Linux.

Arguments

`-w` *work-directory*

Specifies the full path of a work directory that will be used to upgrade the physical host environment for JP1/IM - Manager (Central Scope).

If this option is omitted, `/opt/jp1scope/tmp/` is assumed.

Notes

- You must terminate JP1/IM - Manager before you execute this command. An error results if this command is executed while JP1/IM - Manager is running.
- Before you execute this command, check the available disk space. To execute this command, you need free space equivalent to the size of the monitoring object database. The monitoring object database consists of all data in the following directory:
  `/var/opt/jp1scope/database/jcsdb/`
- Once the `jp1csverup` command has been executed, JP1/IM - Manager (Central Scope) runs under the new version that has been installed, and you can no longer log in from the Monitoring Tree (Editing) window of JP1/IM - View version 08-01 or earlier.

Return values

0	Normal termination
2	Argument error
4	No permission to execute the command
12	Insufficient memory

`13`	Insufficient disk capacity
`31`	Database initialization error
`32`	Data access error
`42`	A service is running
`45`	An attempt was made to execute the command on the new version of the database
`99`	Other error

Examples

Upgrade the physical host environment for the JP1/IM - Manager (Central Scope) that is running under version 08-01; use the `/temp/` work directory:

```
jp1csverup -w /temp
```

Example output

```
The upgrade processing started.
KAVB7750-I Upgrading of the database version has finished.
KAVB7624-I The jcsdbconvert command finished successfully.
The upgrade processing ends successfully.
```

jp1csverup.bat (Windows only)

Function

This command upgrades a physical host environment that has been set up for JP1/IM - Manager (Central Scope) under version 08-01 or earlier. Use this command after you have upgraded your JP1/IM - Manager (Central Scope) from version 08-01 or earlier.

You must execute this command in order to use the functions of a new version of JP1/IM - Manager (Central Scope) that has been installed. However, if you want to use only the functions supported by version 08-01 or earlier, do not execute this command.

Format

```
jp1csverup.bat [-w work-directory]
```

Execution permission

Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Scope-path`\bin\`

Arguments

`-w` *work-directory*

Specifies the full path of a work folder that will be used to upgrade the physical host environment for JP1/IM - Manager (Central Scope). If the path contains a space, enclose the entire path in double-quotation marks (`"`).

If this option is omitted, *Scope-path*`\tmp\` is assumed.

Notes

- You must terminate JP1/IM - Manager before you execute this command. An error results if this command is executed while JP1/IM - Manager is running.
- Before you execute this command, check the available disk space. To execute this command, you need free space equivalent to the size of the monitoring object database. The monitoring object database consists of all data in the following folder:

  Scope-path`\database\jcsdb\`
- Once the `jp1csverup.bat` command has been executed, JP1/IM - Manager (Central Scope) runs under the new version that has been installed, and you can no longer log in from the Monitoring Tree (Editing) window of JP1/IM - View version 08-01 or earlier.

Return values

0	Normal termination
2	Argument error
4	No permission to execute the command
12	Insufficient memory

`13`	Insufficient disk capacity
`31`	Database initialization error
`32`	Data access error
`42`	A service is running
`45`	An attempt was made to execute the command on the new version of the database
`99`	Other error

Examples

Upgrade the physical host environment for the JP1/IM - Manager (Central Scope) that is running under version 08-01; use the `C:\temp` work folder:

```
jp1csverup -w C:\temp
```

Example output

```
The upgrade processing started.
KAVB7750-I Upgrading of the database version has finished.
KAVB7624-I The jcsdbconvert command finished successfully.
The upgrade processing ends successfully.
```

jpc_service

Function

This command turns Setup Enable and disable of add-on program of JP1/IM - Agent.

Format

```
jpc_service {-on | -off} service-name
                   [-h logical-hostname]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linuix:

`/opt/jp1ima/tools/`

Arguments

`-on` *service-name*

Enable add-on program specified in *service-name*.

Logical host's service name is `jpc_`*add-on-directory-name*#`_`*logical-hostname*, but specify `-on` option is `jpc_`*add-on-directory-name*#.

`-off` *service-name*

Disable add-on program specified in *service-name*.

Logical host's service name is `jpc_`*add-on-directory-name*#`_`*logical-hostname*, but specify `-off` option is `jpc_`*add-on-directory-name*#.

`-h` *logical-hostname*

Specifies *logical-hostname* when operating on a cluster system.

#

For the value specified in the *add-on-directory-name*, see *Appendix A.4 (5) About add-on directory names* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Notes

- If the string that you specify in the argument contains spaces or special characters, you must enclose them in " " and escape them.

  In addition, the following characters cannot be used:

  - " (double quotation mark)
  - ! (exclamation)

    - `%` (percent)
    - `^` (circumflex)
- OracleDB exporter cannot be enabled or disabled.

Return values

0	Service Enable activated/deactivated successfully
1	The service is already Enable or disabled.
10	Invalid argument
11	You do not have Execution permissions.
12	Service is running
13	Other commands are executing
251	Service name is invalid
252	Mandatory-services (imagent, imagentproxy, imagentaction) are specified
254	Service definition file not found
255	Failed to activate/deactivate serviced Enable

Log output

- Output destination
  - In Windows:
  Agent-path`\logs\tools\`
  - In Linux:
  `/opt/jp1ima/logs/tools/`

Example

```
jpc_service -on jpc_prometheus
```

jpc_service_autostart

Function

This command setups the automatic startup and shutdown of JP1/IM - Agent.

The service of imagent, imagentproxy, imagentaction and the service of add-on program on which the respective service is add are covered.

For Windows, the service's startup type is setup as follows:

`-on`: Auto

`-off`: Manual

In a clustered environment, Logical host does not allow setup for auto-start and auto-stop because startup and shutdown are controlled by the cluster software.

Format

```
jpc_service_autostart {-on | -off}
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linuix:

`/opt/jp1ima/tools/`

Arguments

`-on`

Enable the auto start of add-on program.

`-off`

Disable the auto start of add-on program.

Notes

- If the string that you specify in the argument contains spaces or special characters, you must enclose them in " " and escape them. In addition, the following characters cannot be used:
  - `"` (double quotation mark)
  - `!` (exclamation)
  - `%` (percent)

    - ^ (circumflex)
- Auto start/stop cannot be set in OracleDB exporter.

Return values

0	Successfully Enable or disable service-auto-start (all succeeded or already Enable or disabled)
10	Invalid argument
11	You do not have Execution permissions.
13	Other commands are executing
255	Failed to activate/deactivate Enable for service auto start

Log output

- Output destination
  - In Windows:
  Agent-path`\logs\tools\`
  - In Linux:
  `/opt/jp1ima/logs/tools/`

Example

```
jpc_service_autostart -on
```

jpc_service_start

Function

This command starts JP1/IM - Agent service.

Format

```
jpc_service_start -s service-key
                        [-h logical-hostname]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linuix:

`/opt/jp1ima/tools/`

Arguments

`-s` *service-key*

Specify the service key.

If "`all`" is specified, all JP1/IM - Agent services are started.

`-h` *logical-hostname*

Specifies logical host name when operating on a cluster system.

Notes

- If the string that you specify in the argument contains spaces or special characters, you must enclose them in `" "` and escape them. In addition, the following characters cannot be used:
  - `"` (double quotation mark)
  - `!` (exclamation)
  - `%` (percent)
  - `^` (circumflex)
- OracleDB exporter cannot be started.

Return values

0	Service started successfully (all successful or already started)
10	Invalid argument
11	You do not have executing permissions.

13	Other commands are executing
251	Service key is invalid
253	Service is not enabled
255	Service failed to start

Log output

- Output destination
  - In Windows:
  Agent-path`\logs\tools\`
  - In Linux:
  `/opt/jp1ima/logs/tools/`

Example

```
jpc_service_start -s all
```

jpc_service_stop

Function

This command stops JP1/IM - Agent service.

Format

```
jpc_service_stop -s service-key
                         [-f]
                         [-h logical-hostname]
```

Execution permission

In Windows: Administrator permissions (if the Windows UAC feature is enabled, the command is executed from the administrator console)

In Linux: Superuser permissions

Storage directory

In Windows:

Agent-path`\tools\`

In Linuix:

`/opt/jp1ima/tools/`

Arguments

`-s` *service-key*

Specify the service key.

If "`all`" is specified, all JP1/IM - Agent services are started.

`-f`

This option forcibly stops the service. Specifies when you want to stop forcibly working service process during cluster operation.

`-h` *logical-hostname*

Specifies logical host name when operating on a cluster system.

Notes

- If the string that you specify in the argument contains spaces or special characters, you must enclose them in " " and escape them. In addition, the following characters cannot be used:
  - " (double quotation mark)
  - `!` (exclamation)
  - `%` (percent)
  - `^` (circumflex)
- OracleDB exporter cannot be stopped.

Return values

0	Service stopped successfully (all successful or already stopped)
10	Invalid argument
11	You do not have execution permissions.
13	Other commands are executing
251	Service key is invalid
253	Service is not enabled
255	Service Failed to Stop

Example

```
jpc_service_stop -s all
```

jpc_stop_node_exporter_aix (AIX only)

Function

This command stops Node exporter for AIX.

The log file of this command is output to the system log of OS.

Format

```
jpc_stop_node_exporter_aix
          [-f]
          [-h logical-hostname]
```

Execution permission

Superuser permissions

Storage directory

It is stored in the directory where Node exporter for AIX archived file (`node_exporter_aix_`*VVRRSS*`.tar.Z`) is extracted.

- When operating on a physical host

```
Any-directory/node_exporter_aix/jp1ima/bin/
```

- When operating on a logical host

```
Shared-directory/node_exporter_aix/jp1ima/bin/
```

Arguments

`-f`

This option forcibly stops the service. Specifies that the service process being started is to be forcibly stopped during cluster operation.

`-h` *logical-hostname*

Specifies the logical host name when operating on a cluster system.

If the logical hostname is 8 bytes or more, in *(1) Enabling registering services* or *(3) Registering the service changed* of *10.4.2 Servicing Node exporter for AIX* in the manual *JP1/Integrated Management 3 - Manager Administration Guide*, specify any character string up to 7 characters specified in the logical host name as `-h` option.

Notes

When operating on a physical host, if the execution path of the `node_exporter_aix` registered to the service is different from the `jpc_stop_node_exporter_aix` command, the `jpc_stop_node_exporter_aix` command terminates normally and the service is stopped, but the `node_exporter_aix` process remains running.

Return values

0	Service stopped successfully (successful or already stopped)
10	Invalid argument

11	You do not have execution permissions.
253	Service is not enabled
255	Service Failed to Stop

Example

```
jpc_stop_node_exporter_aix
```

jr3slget

Function

The `jr3slget` command extracts the system log information of the SAP system.

Format

```
jr3slget    [RFC-connection-information]
            [target-information]
            [-lasttime timestamp-file-name]
            [output-destination]
            [-cnf environment-parameters-file-name]
            [-help]
            [-v]
```

Host that can execute the command

Integrated agent host

Execution permissions

In Windows:

None

In Linux:

None

Storage directory

■Integrated agent host

In Windows:

- For a physical host:

Folder-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Windows*`\sap_windows\command\agtm\evtrap\`

#

Agent-path`\options\sap_windows_`*VVRRSS*`.zip`

In Linux:

- For a physical host:

Directory-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Linux*`/sap_linux/command/agtm/evtrap/`

#

`/opt/jp1ima/options/sap_linux_`*VVRRSS*`.tar.gz`

Arguments

RFC-connection-information

Specifies the information needed to establish RFC connection with the SAP system for command execution.

You can omit specification of this argument if you have specified the RFC connection information in the environment parameters file (`CONNECT` section). If the RFC connection information is specified in both the environment parameters file and the command, the command specification takes effect. For details about the environment parameters file, see *Environment parameters file for jr3slget command (jr3slget.ini)* in *Chapter 2. Definition Files*.

The following describes the RFC information argument:

`-h` *application-server-host-name*

Specifies as 1-100 single-byte alphanumeric characters the name of the connection-target application server host. You must specify one of the following:

- Host name specified in the `hosts` file
- IP address
- SAP router address

You can verify the application server host name by transaction code `SM51`.

When you specify this option, you must also specify the `-s` option.

`-s` *system-number*

Specifies the system number for identification by the application server host specified with the `-h` option. You must specify a value in the range 0-99.

When you specify this option, you must also specify the `-h` option.

`-c` *client-name*

Specifies as 1-3 bytes the client name of the user that is to be used for connection. You must specify a value in the range 0-999.

When you specify this option, you must also specify the `-u` option together with the `-p` or `-p2` option.

`-u` *user-name*

Specifies as 1-12 single-byte alphanumeric characters the user name that is to be used for connection.

When you specify this option, you must also specify the `-c` option together with the `-p` or `-p2` option.

For details about the SAP users that can be specified, see *SAP users used for establishing connection*.

`-p` *password*

Specifies the password for the user specified in the `-u` option. The permitted value is 1-8 single-byte characters.

This option and the `-p2` option are mutually exclusive.

When you specify this option, you must also specify the `-c` and `-u` options.

Specify this option when the SAP system is applying the conventional password rules.

For details about the characters permitted for the password, see *SAP users used for establishing connection*.

`-p2` *extended-password*

Specifies the extended password for the user specified in the `-u` option. The permitted value is 1-40 single-byte characters. This value is case sensitive.

This option and the `-p` option are mutually exclusive.

When you specify this option, you must also specify the `-c` and `-u` options.

Specify this option when the SAP system is applying the extended password rules.

For details about the characters permitted for the extended password, see *SAP users used for establishing connection*.

`-l` *language*

Specifies the language for the user specified with the `-u` option. You must specify a double-byte ISO ID or a single-byte language key used in the SAP system. For example:

- To specify Japanese: `JA`
- To specify a language other than Japanese: `EN`

If you omit this option, the user's language used in the connection-target system is assumed.

When you specify this option, you must also specify the `-c` option, the `-u` option, and the `-p` or `-p2` option.

`-codepage` *code-page*

Specifies the code page to be used when character encoding is converted in the Unicode version of the SAP system.The code page must be specified together with a language in the `-l` option.

Specify the combination of language and code page as shown below. If any other combination of language and code page is specified, an encoding error may occur in the information acquired from the SAP system.

Table 1–54: Combination of language and code page specifications

Connection-target SAP system	Connection language	Language (-l)	Code page (-codepage)
Unicode version	Japanese	JA	`8000`
	English	EN	No need to specify. If you specify a code page, specify `1100`.
Non-Unicode version	Japanese	JA	No need to specify. If you specify a code page, specify `8000`.
	English	EN	No need to specify. If you specify a code page, specify `1100`.

To set the code page to be used to convert character codes at the connection-target SAP system (Unicode version), you can also use the `SAP_CODEPAGE` environment variable provided by the SAP system. If the code page setting is specified in both the `SAP_CODEPAGE` environment variable and in this option, this option takes effect.

If this option is omitted, the connection-target system's default code page is assumed. When you specify this option, you must also specify the `-c` option, the `-u` option, and the `-p` or `-p2` option.

target-information

Specifies information that identifies the system log information that is to be extracted.

You can omit specification of this argument if you have specified the target information in the environment parameters file (`TARGET` section). If target information is specified in both the environment parameters file and the command, the command specification takes effect. For details about the environment parameters file, see *Environment parameters file for jr3slget command (jr3slget.ini)* in *Chapter 2. Definition Files*.

The following describes the target information argument:

`-server` *SAP-instance-name*

Specifies as 1-20 single-byte alphanumeric characters the name of the SAP instance that is collecting system log information. You can specify only one SAP instance name. To check the SAP instance name, use transaction code `SM50` or `SM66`.

`-lasttime` *timestamp-file-name*

If only the system log information that was output after the previous command execution is to be extracted, this option specifies the name of the timestamp file used for managing the previous extraction time.

The permitted value is 1-255 single-byte characters.

If you specify a relative path, make sure that it is relative to the work directory for the command. If you have not specified a work directory for the command in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify the path relative to the current directory.

If you omit this option, the system assumes the period from 00:00:00 to 23:59:59 on the command execution date.

If the specified timestamp file does not exist the first time the command is executed with this argument specified, a new timestamp file is created. System log information is not output during such a first-time execution.

output-destination

Specifies the output destination of the system log information. When you omit this argument, system log information separated by linefeed codes is output to the standard output.

There are two different file formats used by JP1/IM - Agent to output system log information as described below.

- `WRAP1`

  This file is in wraparound format, which means that data is overwritten when the amount of system log Information reaches a specified value. Only one output file can be specified when using this format.

- `WRAP2`

  In this file format, when the amount of system log Information reaches a specified value, data is deleted from the file and then new data is written from the beginning of the file. When the amount of data in the first file reaches a specified value, new data is written in the second file, starting at the top, after all existing data is deleted from the second file. When all of the files are full, new data is again written in the first file, starting at the top, after all existing data is deleted from the first file.

  There can be two through nine output files when using this format. The default is 5 output files. The number of output files is specified in the `NUM` label in the `EXTRACTFILE` section in the environment parameters file.

If you want to change the format of output files, first stop any products monitoring the output files, and then delete the output files and their management files (if there is any).

The following describes the output destination argument:

`-x` *The-name-of-the-storage-file-in-WRAP1-format*

Specifies the relative or full path name of the `WRAP1`-format file to which system log information is to be output. The permitted value is 1 through 251 bytes of single-byte characters.

If you specify a relative path, make sure that it is relative to the work directory for the command. If you have not specified a work directory for the command in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify the path relative to the current directory.

There is a header line of management information at the beginning of this file.

The default file size is 1024 kilobytes. To change the file size, use the `SIZE` label in the `EXTRACTFILE` section of the environment parameters file.

A management file having the name *output-file-name*`.ofs` is created in the same directory as for the output file. For example, if `SYSLOG` is specified as the output file name, a management file named `SYSLOG.ofs` is created in addition to the `SYSLOG` file. If you delete the output file, you must also delete this management file.

The `-x`, `-x2`, and `-xw` options are mutually exclusive.

`-xw` *The-prefix-for-the-storage-files-in-WRAP2-format*

Specifies the name of `WRAP2`-format file in which system log information is to be stored. The permitted value is 1 through 254 bytes of single-byte characters. For the actual file name, a one-byte number is added at the end of the specified file name.

A number in the range from 1 through `NUM` label value is assigned to the specified file name based on the value specified in the `NUM` label in the `EXTRACTFILE` section in the environment parameters file. For example, if `SYSLOG` is specified, storage files `SYSLOG1` through `SYSLOG5` are created by default.

If you specify a relative path, specify a path relative to the command's working directory. If no working directory is specified for commands in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify a path relative to the current directory.

The default file size is 10,240 kilobytes. If you want to change the file size, specify a new size in the `SIZE` label in the `EXTRACTFILE` section in the environment parameters file.

The `-xw`, `-x`, and `-x2` options are mutually exclusive.

-x2

Specifies that system log information is to be output to the file that was specified in the X2PATH label in the EXTRACTFILE section in the environment parameters file.

The -x2, -x, and -xw options are mutually exclusive.

-cnf *environment-parameters-file-name*

Specifies the name of the environment parameters file that is to be referenced by the command. The permitted value is 1-255 bytes of single-byte characters.

If you specify a relative path, make sure that it is relative to the current directory for the command.

If you omit this argument, the system assumes jr3slget.ini, which is the default environment parameters file in the current directory. If there is no default environment parameters file, JP1/IM - Agent assumes the default settings for an environment parameters file.

For details about the environment parameters file and the default settings, see *Environment parameters file for jr3slget command (jr3slget.ini)* in *Chapter 2. Definition Files*.

-help

Specified that the usage of the jr3slget command is to be displayed at the standard output.

-v

Specifies that a message indicating the processing status of the jr3slget command is to be output to the standard output. If you omit this option, no message indicating the processing status of the command will be output.

SAP users used for establishing connection

To collect system log information, the jr3slget command executes the external management interfaces defined in the SAP system using RFC (communication protocol of SAP AG). Therefore, you must provide in advance the users who are to be used by the jr3slget command for establishing connection in the SAP system. This subsection describes the user types, passwords, and authorizations for the SAP users who are created in the SAP system.

User types

The following types of SAP users can be used by JP1/IM - Agent:

- Dialog
- System
- Communication
- Service

Characters permitted for passwords

Define passwords for the SAP users. A password can consist of single-byte numeric characters (from 0 to 9), single-byte alphabetic characters (from a to z, A to Z), and the following single-byte symbols:

!, @, $, %, &, /, (,), =, ?, ', `, *, +, ~, #, -, _, ., :, {, [,], }, <, >, |

Required authorizations

You must set the following authorizations (authorization objects) for the users:

- Authorizations required for a user to establish RFC connection with function modules (S_RFC)
- Authorizations required in order to use external management interfaces (S_XMI_PROD)

For the value of each authorization, assign a value shown in the tables below or use the built-in configurations (S_RFC_ALL and S_XMI_ADMIN) that specify an asterisk (*) for all items.

Table 1–55: Authorizations required for a user to establish RFC connection with function modules (S_RFC)

Authorization	Description	Value
RFC_TYPE	Type of RFC object to be protected	FUGR (function group)
RFC_NAME	RFC name to be protected	*
ACTVT	Activity	16 (execution)

Table 1–56: Authorizations required in order to use external management interfaces (S_XMI_PROD)

Authorization	Description	Value
EXTCOMPANY	Company name of the external management tool	HITACHI
EXTPRODUCT	Program name of the external management tool	JP1
INTERFACE	Interface ID	*

Note

To use the remote monitoring function, you have to specify information (host name, instance name, etc.) regarding the SAP system to be monitored for the following settings: the RFC connection information or target information to be specified as a command argument, and the CONNECT section in the environment parameters file.

Output format and contents

The command extracts the system log information (including parameter record rows) that can be verified by transaction code SM21 in the SAP system.

The following is the default output format for system log information, where < > enclose a field ID:

```
<TIME><INSTANCE><USER><PROGRAM><MSGNO><MSGTEXT>
```

If the value of a system log information item is shorter than the predefined field length, the remaining area is padded with single-byte spaces. The following table lists and explains the values that are output:

Table 1–57: System log information that is output

Field ID	Description	Length (bytes)
<TIME>	Time the message was recorded (*HH:MM:SS*)	8
<INSTANCE>	Server that recorded the message	20
<USER>	User who recorded the message	12
<PROGRAM>	Program that recorded the message	8
<MSGNO>	Message number	3
<MSGTEXT>	Message text	255

Return value

0	Normal termination

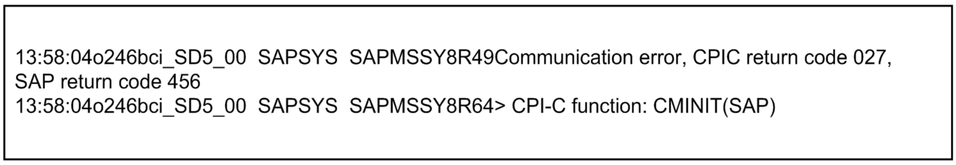
1 or greater	Abnormal termination

Example

This example outputs the system log information for the o246bci_SD5_00 SAP instance. The RFC connection information has already been defined in the environment parameters file.

```
jr3slget -server o246bci_SD5_00
```

The output example from this command is as follows:



```
13:58:04o246bci_SD5_00  SAPSYS  SAPMSSY8R49Communication error, CPIC return code 027,
SAP return code 456
13:58:04o246bci_SD5_00  SAPSYS  SAPMSSY8R64> CPI-C function: CMINIT(SAP)
```

jr3alget

Function

The `jr3alget` command extracts the CCMS alert information of the SAP system.

Format

```
jr3alget    [RFC-connection-information]
            [target-information]
            [-lasttime timestamp-file-name]
            [output-destination]
            [-cnf environment-parameters-file-name]
            [-help]
            [-v]
```

Host that can execute the command

Integrated agent host

Execution permissions

In Windows:

None

In Linux:

None

Storage directory

■Integrated agent host

In Windows:

- For a physical host:

Folder-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Windows*`\sap_windows\command\agtm\evtrap\`

#

Agent-path`\options\sap_windows_`*VVRRSS*`.zip`

In Linux:

- For a physical host:

Directory-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Linux*`/sap_linux/command/agtm/evtrap/`

#

`/opt/jp1ima/options/sap_linux_`*VVRRSS*`.tar.gz`

Arguments

RFC-connection-information

Specifies the information needed to establish RFC connection with the SAP system for command execution.

You can omit specification of this argument if you have specified the RFC connection information in the environment parameters file (`CONNECT` section). If the RFC connection information is specified in both the environment parameters file and the command, the command specification takes effect. For details about the environment parameters file, see *Environment parameters file for jr3alget command (jr3alget.ini)* in *Chapter 2. Definition Files*.

The following describes the RFC information argument:

`-h` *application-server-host-name*

Specifies as 1-100 single-byte alphanumeric characters the name of the connection-target application server host. You must specify one of the following:

- Host name specified in the `hosts` file
- IP address
- SAP router address

You can verify the application server host name by transaction code `SM51`.

When you specify this option, you must also specify the `-s` option.

`-s` *system-number*

Specifies the system number for identification by the application server host specified with the `-h` option. You must specify a value in the range 0-99.

When you specify this option, you must also specify the `-h` option.

`-c` *client-name*

Specifies as 1-3 bytes the client name of the user that is to be used for connection. You must specify a value in the range 0-999.

When you specify this option, you must also specify the `-u` option together with the `-p` or `-p2` option.

`-u` *user-name*

Specifies as 1-12 single-byte alphanumeric characters the user name that is to be used for connection.

When you specify this option, you must also specify the `-c` option together with the `-p` or `-p2` option.

For details about the SAP users that can be specified, see *SAP users used for establishing connection*.

`-p` *password*

Specifies the password for the user specified in the `-u` option. The permitted value is 1-8 single-byte characters.

This option and the `-p2` option are mutually exclusive.

When you specify this option, you must also specify the `-c` and `-u` options.

Specify this option when the SAP system is applying the conventional password rules.

For details about the characters permitted for the password, see *SAP users used for establishing connection*.

`-p2` *extended-password*

Specifies the extended password for the user specified in the `-u` option. The permitted value is 1-40 single-byte characters. This value is case sensitive.

This option and the `-p` option are mutually exclusive.

When you specify this option, you must also specify the `-c` and `-u` options.

Specify this option when the SAP system is applying the extended password rules.

For details about the characters permitted for the extended password, see *SAP users used for establishing connection*.

`-l` *language*

Specifies the language for the user specified with the `-u` option. You must specify a double-byte ISO ID or a single-byte language key used in the SAP system. For example:

- To specify Japanese: JA
- To specify a language other than Japanese: EN

If you omit this option, the user's language used in the connection-target system is assumed.

When you specify this option, you must also specify the -c option, the -u option, and the -p or -p2 option.

-codepage *code-page*

Specifies the code page to be used when character encoding is converted in the Unicode version of the SAP system.

The code page must be specified together with a language in the -l option.

Specify the combination of language and code page as shown below. If any other combination of language and code page is specified, an encoding error may occur in the information acquired from the SAP system.

Table 1–58: Combination of language and code page specifications

Connection-target SAP system	Connection language	Language (-l)	Code page (-codepage)
Unicode version	Japanese	JA	8000
	English	EN	No need to specify. If you specify a code page, specify 1100.
Non-Unicode version	Japanese	JA	No need to specify. If you specify a code page, specify 8000.
	English	EN	No need to specify. If you specify a code page, specify 1100.

To set the code page to be used to convert character codes at the connection-target SAP system (Unicode version), you can also use the SAP_CODEPAGE environment variable provided by the SAP system. If the code page setting is specified in both the SAP_CODEPAGE environment variable and in this option, this option takes effect.

If this option is omitted, the connection-target system's default code page is assumed.When you specify this option, you must also specify the -c option, the -u option, and the -p or -p2 option.

target-information

Specifies information that identifies the CCMS alert information that is to be extracted.

You can omit specification of this argument if you have specified the target information in the environment parameters file (TARGET section). If target information is specified in both the environment parameters file and the command, the command specification takes effect. For details about the environment parameters file, see *Environment parameters file for jr3alget command (jr3alget.ini)* in *Chapter 2. Definition Files*.

The following describes the target information argument:

-ms *monitor-set-name*

Specifies as 1-60 single-byte alphanumeric characters the monitor set name. The monitor set name is displayed as CCMS monitor set on the Alert Monitor (transaction code RZ20) of the SAP system.

When you specify this option, you must also specify the -mn option.

-mn *monitor-name*

Specifies as 1-60 single-byte alphanumeric characters the monitor name defined in the monitor set. The monitor name is displayed in the tree of the CCMS monitor set on the Alert Monitor (transaction code RZ20) of the SAP system.

When you specify this option, you must also specify the -ms option.

-lasttime *timestamp-file-name*

If only the CCMS alert information that was output after the previous command execution is to be extracted, this option specifies the name of the timestamp file used for managing the previous extraction time.

The permitted value is 1-255 single-byte characters.

If you specify a relative path, make sure that it is relative to the work directory for the command. If you have not specified a work directory for the command in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify the path relative to the current directory.

If you omit this option, the system assumes the period from 00:00:00 to 23:59:59 on the command execution date.

If the specified timestamp file does not exist the first time the command is executed with this argument specified, a new timestamp file is created. CCMS alert information is not output during such a first-time execution.

output-destination

Specifies the output destination of the CCMS alert information. When you omit this argument, CCMS alert information separated by linefeed codes is output to the standard output.

There are two different file formats used by JP1/IM - Agent to output CCMS Alert Information as described below.

- `WRAP1`

  This file is in wraparound format, which means that data is overwritten when the amount of CCMS Alert Information reaches a specified value. There can be only one output file when using this format.

- `WRAP2`

  In this file format, when the amount of CCMS Alert Information reaches a specified value, all data is deleted from the file and then new data is written from the beginning of the file. When the amount of data in the first file reaches a specified value, new data is written in the second file, starting at the top, after all existing data is deleted from the second file. When all of the files are full, new data is again written in the first file, starting at the top, after all existing data is deleted from the first file.

  There can be two through nine output files when using this format. The default is 5 output files. The number of output files is specified in the `NUM` label in the `EXTRACTFILE` section in the environment parameters file.

If you want to change the format of output files, first stop any products monitoring the output files, and then delete the output files and their management files (if there is any).

The following describes the output destination argument:

`-x` *The-name-of-the-storage-file-in-WRAP1-format*

Specifies the relative or full path name of the `WRAP1`-format file in which CCMS Alert Information is to be stored. The permitted value is 1 through 251 bytes of single-byte characters.

If you specify a relative path, make sure that it is relative to the work directory for the command. If you have not specified a work directory for the command in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify the path relative to the current directory.

There is a header line of management information at the beginning of this file.

The default file size is 1,024 kilobytes. To change the file size, use the `SIZE` label in the `EXTRACTFILE` section of the environment parameters file.

A management file having the name *storage-file-name*`.ofs` is created in the same directory as for the storage file. For example, if `ALERT` is specified as the storage file name, a management file named `ALERT.ofs` is created in addition to the `ALERT` file. If you delete the storage file, you must also delete this management file.

The `-x`, `-x2`, and `-xw` options are mutually exclusive.

`-xw` *The-prefix-for-the-storage-files-in-WRAP2-format*

Specifies the name of `WRAP2`-format file in which CCMS Alert Information is to be stored. The permitted value is 1 through 254 bytes of single-byte characters. For the actual file names, a one-byte number is added at the end of the specified file name.

A number in the range from 1 through the `NUM` label value is assigned to the specified file name based on the value specified in the `NUM` label in the `EXTRACTFILE` section in the environment parameters file. For example, if `ALERT` is specified, storage files `ALERT1` through `ALERT5` are created by default.

If you specify a relative path, specify a path relative to the command's working directory. If no working directory is specified for commands in the `WORKDIR` label of the `COMMAND` section in the environment parameters file, specify a path relative to the current directory.

The default file size is 10,240 kilobytes. If you want to change the file size, specify a new size in the `SIZE` label in the `EXTRACTFILE` section in the environment parameters file.

The `-xw`, `-x`, and `-x2` options are mutually exclusive.

`-x2`

Specifies that CCMS Alert Information is to be output to the file that was specified in the `X2PATH` label in the `EXTRACTFILE` section in the environment parameters file.

The `-x2`, `-x`, and `-xw` options are mutually exclusive.

`-cnf` *environment-parameters-file-name*

Specifies the name of the environment parameters file that is to be referenced by the command. The permitted value is 1-255 bytes of single-byte characters.

If you specify a relative path, make sure that it is relative to the current directory for the command.

If you omit this argument, the system assumes `jr3alget.ini`, which is the default environment parameters file in the current directory. If there is no default environment parameters file, JP1/IM - Agent assumes the default settings for an environment parameters file.

For details about the environment parameters file and the default settings, see *Environment parameters file for jr3alget command (jr3alget.ini)* in *Chapter 2. Definition Files*.

`-help`

Specifies that the usage of the `jr3alget` command is to be displayed at the standard output.

`-v`

Specifies that a message indicating the processing status of the `jr3alget` command is to be output to the standard output. If you omit this option, no message indicating the processing status of the command will be output.

SAP users used for establishing connection

To collect CCMS alert information, the `jr3alget` command executes the external management interfaces defined in the SAP system using RFC (communication protocol of SAP AG). Therefore, you must provide in advance the users who are to be used by the `jr3alget` command for establishing connection in the SAP system. This subsection describes the user types, passwords, and authorizations for the SAP users who are created in the SAP system.

User types

The following types of SAP users can be used by JP1/IM - Agent:

- Dialog
- System
- Communication
- Service

Characters permitted for passwords

Define passwords for the SAP users. A password can consist of single-byte numeric characters (from `0` to `9`), single-byte alphabetic characters (from `a` to `z`, `A` to `Z`), and the following single-byte symbols:

```
!, @, $, %, &, /, (, ), =, ?, ', `, *, +, ~, #, -, _, ., :, {, [, ], }, <, >, |
```

Required authorizations

You must set the following authorizations (authorization objects) for the users:

- Authorizations required for a user to establish RFC connection with function modules (S_RFC)
- Authorizations required in order to use external management interfaces (S_XMI_PROD)

For the value of each authorization, assign a value shown in the tables below or use the built-in configurations (S_RFC_ALL and S_XMI_ADMIN) that specify an asterisk (*) for all items.

Table 1–59: Authorizations required for a user to establish RFC connection with function modules (S_RFC)

Authorization	Description	Value
RFC_TYPE	Type of RFC object to be protected	FUGR (function group)
RFC_NAME	RFC name to be protected	*
ACTVT	Activity	16 (execution)

Table 1–60: Authorizations required in order to use external management interfaces (S_XMI_PROD)

Authorization	Description	Value
EXTCOMPANY	Company name of the external management tool	HITACHI
EXTPRODUCT	Program name of the external management tool	JP1
INTERFACE	Interface ID	*

Notes

- Because the CCMS alert information is treated as an SAP system resource and can be referenced from any application server, the connection target can be any application server. Make sure that only one command is executed per SAP system.
- To use the remote monitoring function, you have to specify information (host name, instance name, etc.) regarding the SAP system to be monitored for the following settings: the RFC connection information or target information to be specified as a command argument, and the CONNECT section in the environment parameters file.

Output format and contents

The following is the default output format for CCMS alert information, where < > enclose a field ID:

```
<ALERTDATE><ALERTTIME><MTSYSID><MTMCNAME><OBJECTNAME><FIELDNAME><VALUE><SEVERITY><MSG>
```

If the value of a CCMS alert information item is shorter than the predefined field length, the remaining area is padded with single-byte spaces. The following table lists and explains the values that are output:

Table 1–61: CCMS alert information that is output

Field ID	Description	Source	Length (bytes)
<ALSYSID>	Name of the SAP system	Alert ID (AID) (BAPIAID)	8
<MSEGNAME>	Name of the monitoring segment		40

Field ID	Description	Source	Length (bytes)
`<ALUNIQNUM>`	Unique ID used by `AID`		10
`<ALERTDATE>`	Date the alert occurred (*YYYYMMDD*)		8
`<ALERTTIME>`	Time the alert occurred (*HHMMSS*)		6
`<MTSYSID>`	Name of the SAP system	ID of the MTE associated with the alert (`TID`) (`BAPITID`)	8
`<MTCLASS>`	MTE type		3
`<MTNUMRANGE>`	Range of numbers (such as resident or temporary)		3
`<MTMCNAME>`	Name of the monitoring context		40
`<MTUID>`	Unit ID used by `TID`		10
`<VALUE>`	Warning value (corresponding to the color of the CCMS alert entry that can be viewed with transaction code `RZ20`): • `0`: Gray (invalid information) • `1`: Green (OK) • `2`: Yellow (warning) • `3`: Red (problem or error)	Alert severity level (`BAPIALDATA`)	11
`<SEVERITY>`	Severity level (0-255; severity increases as the value increases)		
`<FIELDNAME>`	Abbreviation of MTE	General property (`BAPIALERT`)	40
`<STATUS>`	Alert status		11
`<OBJECTNAME>`	Name of the monitoring object		40
`<MANDT>`	Client		3
`<USERID>`	SAP user		12
`<REPORTEDBY>`	Reporter (logical name)		16
`<STATCHGDAT>`	Last date the status changed		8
`<STATCHGBY>`	Last user who changed the status (logical name)		16
`<STATCHGTIM>`	Last time the status changed		6
`<MSCGLID>`	Message ID when a message with the log attribute activated an alert		50
`<MSGCLASS>`	Message recorder	Message	16
`<MSGID>`	Message ID		30
`<MSGARG1>`	Character string for message insert word 1		128
`<ARGTYPE1>`	Type of message insert word 1		1
`<MSGARG2>`	Character string for message insert word 2		128
`<ARGTYPE2>`	Type of message insert word 2		1

Field ID	Description	Source	Length (bytes)
`<MSGARG3>`	Character string for message insert word 3		128
`<ARGTYPE3>`	Type of message insert word 3		1
`<MSGARG4>`	Character string for message insert word 4		128
`<ARGTYPE4>`	Type of message insert word 4		1
`<MSGTEXT>`	Message text		128
`<MSG>`	Translated message		255

Return value

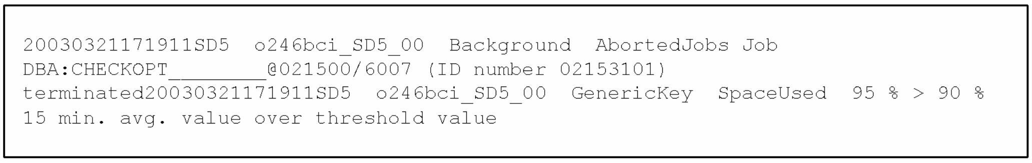
`0`	Normal termination
`1` or greater	Abnormal termination

Example

This example outputs CCMS alert information using `SAP CCMS Monitor Templates` as the monitor set name and `Entire System` as the monitor name. The RFC connection information has already been defined in the environment parameters file.

```
jr3alget -ms "SAP CCMS Monitor Templates" -mn "Entire System"
```

The output example from this command is as follows:



```
20030321171911SD5  o246bci_SD5_00  Background  AbortedJobs Job
DBA:CHECKOPT________@021500/6007 (ID number 02153101)
terminated20030321171911SD5  o246bci_SD5_00  GenericKey  SpaceUsed  95 % > 90 %
15 min. avg. value over threshold value
```

promtool

Function

This command checks the format of Prometheus server definition files and tests alert rules.

Format

```
promtool check config Prometheus-configuration-file-name
         check rules alert-configuration-file-name
         test rules test-file-name ...
```

Execution permission

None

Storage directory

In Windows:

Agent-path`\tools\`

In Linuix:

`/opt/jp1ima/tools/`

Arguments

`check config` *Prometheus-configuration-file-name*

Check the format of the Prometheus configuration file for errors.

For details about the Prometheus configuration file, see *Prometheus configuration file (jpc_prometheus_server.yml)*.

`check rules` *alert-configuration-file-name*

Check for errors in the format of the alert configuration file.

For details about the alert configuration file, see *Alert configuration file (jpc_alerting_rules.yml)*.

`test rules` *test-file-name* `...`

Run a test of the alert rule that you wrote in the test file. You can specify up to 10 test files.

Return values

0	Format is correct, and alert rule test successful.
other than 0	Format is incorrect, and alert rule test failure.

Alert rule test file contents

Format

Write in YAML format.

File

Any-name`.yml`

Description

Item name	Description	Default value
rule_files: [- <file_name>]	Specify a list of rule files to consider for testing. The file name can be specified as a wildcard.	--
[evaluation_interval: <duration> | default = 1m]	Specify the evaluation interval for the alert rule.	1m

group_eval_order:
[- <group_name>]
	You can specify the order of group names.
	The order of the group names is the order in which the rule groups are evaluated (specific evaluation times). The order specified is guaranteed only for the group name described.
	You don't have to describe every group.
	You can specify the evaluation order of the rule file described in `rule_files:`, as shown in the following example.
	<Description example>
	`group_eval_order:`
	`- test02.yml`
	`- test01.yml`
		--

tests: [- <test_group>]	Enumerate all tests.	--

Legend:

--: Not applicable

- <test_group>

Item name	Description	Default value
interval: <duration>	Specify the interval between data occurrences for `input_series:`.	--
input_series: [- <series>]	Specify the data for the series.	--
[name: <string>]	Specify a name for the <test group>.	--
alert_rule_test: [- <alert_test_case>]	Specify a test for the alert rule. Considers the alert rule from the specified file.	--

Legend:

--: Not applicable

- <series>

Item name	Description	Default value

series: <string>	Specify the data for the series in the following format:
	`'`*metric-name* `{`*label-name* `=` *label-value*`, ...}'`
	<Description example>
	series_name{label1="value1", label2="value2"}
	go_goroutines{job="prometheus", instance="localhost:9090"}
		--

values: <string>	Specify the data to occur, separated by spaces. You can use the following expansion notation: <Example of expanded notation> 'a+bxc' becomes 'a a+b a+(2*b) a+(3*b) ... a+(c*b)' 'a-bxc' becomes 'a a-b a-(2*b) a-(3*b) ... a-(c*b)' <Description example> '-2+4x3' becomes '-2 2 6 10'	--

Item name	Description	Default value
	' 1-2x4' becomes '1 -1 -3 -5 -7'	

Legend:

--: Not applicable

- <alert_test_case>

Item name	Description	Default value
eval_time: <duration>	Specify the time elapsed since "`time = 0s`" when to evaluate the test (check for alerts). Evaluates the data occurrence interval specified in `interval:` in <test_group> up to the elapsed time specified in `eval_time:`. For example, if the data occurrence interval specified for `interval:` in <test_group> is `1m` and the elapsed time specified for `eval_time:` is `5m`, it is evaluated when the sixth data specified in `input_series:` is acquired.	--
alertname: <string>	Specifies the name of the alert to test. Specify the value described in `alert:` in the alert configuration file.	--
exp_alerts: [- <alert>]	Specify a list of alerts that you expect to raise. If you want to test that the alert rule does not run, leave the `exp_alerts` specification empty.	--

Legend:

--: Not applicable

- <alert>

Item name	Description	Default value
exp_labels: [<labelname>: <string>]	Specifies the label of the alert that you expect to raise. The label also includes the label of the sample associated with the alert.	--
exp_annotations: [<labelname>: <string>]	Specifies the annotation of the alert that you expect to raise.	--

Legend:

--: Not applicable

Sample alert configuration file and alert rule test file

- Examples of "up" metrics

- Example of description of alert configuration file

```
groups:
- name: alerts
  rules:

  - alert: InstanceDown
    expr: up == 0
    for: 5m
    labels:
        severity: page
    annotations:
        summary: "Instance {{ $labels.instance }} down"
        description: "{{ $labels.instance }} of job {{ $labels.job }} has
been down for more than 5 minutes."
```

- Example of description of alert rule test file

```
rule_files:
    - jpc_alerting_rules.yml

evaluation_interval: 1m

tests:
    # Test
    - interval: 1m
      # Series data.
      input_series:
          - series: 'up{job="prometheus", instance="localhost:9090"}'
            values: '0 0 0 0 0 0 0 0 0 0 0 0 0 0 0' # success

      # Unit test for alerting rules.
      alert_rule_test:
          # Unit test 1.
          - eval_time: 5m
            alertname: InstanceDown
            # alertname: AnotherInstanceDown
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      severity: page
                      instance: localhost:9090
                      job: prometheus
                  exp_annotations:
                      summary: "Instance localhost:9090 down"
                      description: "localhost:9090 of job prometheus has b
een down for more than 5 minutes."
```

- Examples of CPU

- Example of description of alert configuration file

```
groups:
  - name: alerts
    rules:
      - alert: cpu_alert_rule
        expr: sum(rate(windows_cpu_time_total{mode!="idle"}[1m])) < 50
        for: 2m
        labels:
          severity: page
        annotations:
          summary: "CPU alert rule summary"
          description: "CPU alert rule description"
```

- Example of description of alert rule test file

```
rule_files:
    - jpc_alerting_rules.yml

evaluation_interval: 1m
```

```
tests:
    # Test
    - interval: 1m
      # Series data.
      input_series:
          - series: 'windows_cpu_time_total'
            #values: '0+3000x10' # fail
            values: '0+2800x10'  # success

      # Unit test for alerting rules.
      alert_rule_test:
          # Unit test 1.
          - eval_time: 7m
            alertname: cpu_alert_rule
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      severity: page
                  exp_annotations:
                      summary: "CPU alert rule summary"
                      description: "CPU alert rule description"
```

- Examples of memory (#1)

- Example of description of alert configuration file

```
groups:
  - name: alerts
    rules:
      - alert: memory_alert_rule
        expr: windows_memory_available_bytes < 1073741824
        for: 3m
        labels:
          severity: page
        annotations:
          summary: "Memory alert rule summary"
          description: "Memory alert rule description"
```

- Example of description of alert rule test file

```
rule_files:
    - jpc_alerting_rules.yml

evaluation_interval: 1m

tests:
    # Test
    - interval: 1m
      # Series data.
      input_series:
          - series: 'windows_memory_available_bytes'
            values: '1073741822 1073741826 1073741823 1073741823 107374182
3 1073741823 1073741828 1073741822' # success
            #values: '1073741822 1073741822 1073741826 1073741823 10737418
23 1073741823 1073741828 1073741822' # fail

      # Unit test for alerting rules.
      alert_rule_test:
          # Unit test 1.
          - eval_time: 5m
            alertname: memory_alert_rule
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      severity: page
                  exp_annotations:
                      summary: "Memory alert rule summary"
                      description: "Memory alert rule description"
```

- Examples of memory (#2)

- Example of description of alert configuration file

```
groups:
  - name: alerts
    rules:
      - alert: memory_alert_rule
        expr: windows_memory_available_bytes < 1073741824
        for: 3m
        labels:
          severity: page
        annotations:
          summary: "Memory alert rule summary"
          description: "Memory alert rule description"
```

- Example of description of alert rule test file

```
rule_files:
    - jpc_alerting_rules.yml

evaluation_interval: 1m

tests:
    # Test
    - interval: 1m
      # Series data.
      input_series:
          - series: 'windows_memory_available_bytes'
            values: '1073741822 1073741826 1073741823 1073741823 107374182
3 1073741823 1073741828 1073741822' # success
            #values: '1073741822 1073741822 1073741826 1073741823 10737418
23 1073741823 1073741828 1073741822' # fail

      # Unit test for alerting rules.
      alert_rule_test:
          # Unit test 1.
          - eval_time: 5m
            alertname: memory_alert_rule
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      severity: page
                  exp_annotations:
                      summary: "Memory alert rule summary"
                      description: "Memory alert rule description"
```

- **Examples of interrupt**

- Example of description of alert configuration file

```
groups:
  - name: alerts
    rules:
      - alert: alerts_rules_increase
        expr: increase(windows_cpu_interrupts_total{core="0,0"}[3m]) > 100
        for: 0m
        labels:
          severity: critical
        annotations:
          summary: "Alert test case of increase."
          description: "Use increase function in unit test."

      - alert: alerts_rules_increase_all
        expr: sum(increase(windows_cpu_interrupts_total[5m])) > 240
        for: 0m
        labels:
          severity: critical
        annotations:
          summary: "Alert test case of increase."
          description: "Use increase function in unit test."
```

- Example of description of alert rule test file

```
rule_files:
    - jpc_alerting_rules.yml

evaluation_interval: 1m

tests:
    # Test
    - interval: 1m
      # Series data.
      input_series:
          - series: 'windows_cpu_interrupts_total{core="0,0"}'
            #values: '0 10 20 30 110 120 130 140 150 160 170' #fail
            values: '0+10x3 111+10x6'  #success
          - series: 'windows_cpu_interrupts_total{core="0,1"}'
            values: '0+10x3 98+13x6'

      # Unit test for alerting rules.
      alert_rule_test:
          # Unit test 1.
          - eval_time: 4m
            alertname: alerts_rules_increase
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      core: "0,0"
                      severity: critical
                  exp_annotations:
                      summary: "Alert test case of increase."
                      description: "Use increase function in unit test."
          - eval_time: 8m
            alertname: alerts_rules_increase_all
            exp_alerts:
                # Alert 1.
                - exp_labels:
                      severity: critical
                  exp_annotations:
                      summary: "Alert test case of increase."
                      description: "Use increase function in unit test."
```

Examples

- Example of performing a format check on a Prometheus configuration file (if the format is correct)

```
# ./promtool check config jpc_prometheus_server.yml
Checking jpc_prometheus_server.yml
  SUCCESS: 1 rule files found

Checking jpc_alerting_rules.yml
  SUCCESS: 1 rules found
```

- Example of performing a format check on a Prometheus configuration file (if the format is incorrect)

```
# ./promtool check config jpc_prometheus_server.yml
Checking jpc_prometheus_server.yml
  FAILED: parsing YAML file jpc_prometheus_server.yml: yaml: line 42: did
not find expected key
```

- Example of performing a format check of the alert configuration file (if the format is correct)

```
# ./promtool check rules jpc_alerting_rules.yml
Checking jpc_alerting_rules.yml
  SUCCESS: 1 rules found
```

- Example of performing a format check of the alert configuration file (if the format is incorrect)

```
# ./promtool check rules jpc_alerting_rules.yml
Checking jpc_alerting_rules.yml
  FAILED:
jpc_alerting_rules.yml: yaml: unmarshal errors:
  line 10: field aannotations not found in type rulefmt.RuleNode
```

- Example of running an alert rule test (if the test is successful)

```
# ./promtool test rules alerts_rules_unit_test.yml
Unit Testing:  alerts_rules_unit_test.yml
  SUCCESS
```

- Example of running an alert rule test (if the test fails (Part 1))

```
# ./promtool test rules alerts_rules_unit_test.yml
Unit Testing:  alerts_rules_unit_test.yml
  FAILED:
    alertname:InstanceDown, time:10m,
        exp:"[Labels:{alertname=\"InstanceDown\", instance=\"localhost:909
0\", job=\"prometheus\", severity=\"page\"} Annotations:{description=\"loc
alhost:9090 of job prometheus has been down for more than 5 minutes.\", su
mmary=\"Instance localhost:9090 down\"}]",
        got:"[]
```

If the test file is invalid, an alert that is expected to occur in exp and an alert that actually occurs in got are output. In the case of the above execution example, it indicates that no alert was actually notified (output result of got) for the expectation that one alert is output (output result of exp).

- Example of running an alert rule test (if the test fails (Part 2))

```
# ./promtool test rules test_rule_file.yml
Unit Testing:  test_rule_file.yml
  FAILED:
    alertname:InstanceDown, time:5m,
        exp:"[Labels:{alertname=\"InstanceDown\", instance=\"localhost:909
0\", job=\"prometheus\", severity=\"warn\"} Annotations:{description=\"loc
alhost:9090 of job prometheus has been down for more than 5 minutes.\", su
mmary=\"Instance localhost:9090 down\"}]",
        got:"[Labels:{alertname=\"InstanceDown\", instance=\"localhost:909
0\", job=\"prometheus\", severity=\"page\"} Annotations:{description=\"loc
alhost:9090 of job prometheus has been down for more than 5 minutes.\", su
mmary=\"Instance localhost:9090 down\"}]
```

If the test file is invalid, an alert that is expected to occur in exp and an alert that actually occurs in got are output. In the above execution example, it is assumed that the value of severity is warn (output result of exp), but the value of severity is actually page (output result of got).

SpmSetSvcCon (Windows only)

Function

This command sets or cancels dependencies between the JP1/IM-Manager service and the JP1/Base Event service. If only JP1/IM - Manager needs to be deleted from a logical host, this command can also delete only the JP1/IM-Manager service on the logical host.

Format

```
SpmSetSvcCon {-setdepend {yes|no} | -d -h logical-host-name}
```

Execution permission

Administrator permissions (If the Windows UAC feature is enabled, the command is executed from the administrator console)

Storage directory

Console-path`\bin\`

Arguments

`-setdepend {yes|no}`

Sets the dependencies for a registered service.

- `yes`: Sets the dependencies between the JP1/IM-Manager service and the JP1/Base Event service.
- `no`: Cancels the dependencies between the JP1/IM-Manager service and the JP1/Base Event service.

`-d -h` *logical-host-name*

Specify this option to delete only JP1/IM - Manager from a logical host. For details about the procedure for deleting only JP1/IM - Manager from a logical host, see *7.7.1(4) Deleting only JP1/IM - Manager and IM databases on a logical host* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Return values

`0`	Normal termination
`1`	Argument error
`2`	Execution permission error
`3`	The JP1/IM-Manager service is not registered
`255`	Other error

2 Definition Files

This chapter describes the format and syntax of JP1/IM definition files.

List of definition files

The following table lists the JP1/Integrated Management definition files.

List of definition files

Table 2–1: List of definition files

Product name		Definition file name	Description
JP1/Base		Configuration definition file	Defines the system hierarchy that is to be managed by JP1/IM. For details about the configuration definition file (`jbs_route.conf`), see the *JP1/Base User's Guide*.
		Environment variable file[#3]	Defines environment variables to be used when commands are executed at managed hosts in JP1/IM. For details about the environment variable file, see the *JP1/Base User's Guide*.
		Host group definition file	Defines a group of managed hosts in JP1/IM. For details about the host group definition file, see the *JP1/Base User's Guide*.
JP1/IM - Manager	JP1/IM - Manager	Common definition settings file (changing the attribute of JP1 events)	Changes the attribute of JP1 events.
		Operation log definition file (`imm_operationlog.conf`)	Defines whether to output operation log data, the output destination, log file size, and number of files.
	Intelligent Integrated Management Base	Intelligent Integrated Management Base definition file (`imdd.properties`)	Defines system settings for the Intelligent Integrated Management Base.
		System node definition file (`imdd_systemnode.conf`)[#3]	Contains settings to define the hierarchical structure of the system to represent the structure in a sunburst or tree chart, and settings to group collected data into defined hosts.
		Category name definition file for IM management nodes (`imdd_category_name.conf`)[#3]	Defines IM management node category names for management groups to be displayed in a sunburst or tree chart.
		Target host definition file for configuration collection (`imdd_target_host.conf`)[#3]	Defines the hosts from which to collect information regarding monitoring objects of each linked product.
		Host name definition file (`imdd_host_name.conf`)[#3]	Defines mapping between aliases and real host names.
		IM management node link definition file (`imdd_nodeLink_def.conf`)[#3]	Defines relationships between IM management nodes.
		Suggestion definition file (`imdd_suggestion.conf`)[#3]	Defines criteria for suggesting response actions and what the actions do, which are used by the suggestion function.
		Suggestion definition file (user-created) (`imdd_suggestion_`*any-file-name*`.conf`)[#3,#4]	
		Single sign-on mapping definition file (`imdd_sso_mapping.properties`)[#3]	Defines the mapping between the name of the JP1 user used in the Intelligent Integrated Management Base and the name of the user registered in the OpenID provider.

Product name		Definition file name	Description
		Auto response action definition file (`autoactconf.json`) #3	A file that restores execution conditions in Automatic Response Action and Automatic Response Action definition, which is executed contents are recorded.
		Response action state monitoring definition file (`responseactionnotice.conf`)	A file that defines setup for monitoring execute status for automated Response Action.
		User-created definition file list definition file (`imdd_user_deffile_list.json`)#3	A file that defines a user-created file that can be updated or delete with the functions provided by JP1/IM - Manager.
		Definition file properties file (`imdd_file_properties.json`)	This File defines file name, file path, and the operation for importing the definition file when acquiring or updating the definition file.
	Central Console	Event-source-host mapping definition file (`user_hostmap.conf`) #3	Defines mapping on the event source host.
		Automated action environment definition file (`action.conf.update`)	Defines an execution environment for automated actions.
		Automated action definition file (`actdef.conf`)	Defines conditions for executing an automated action and the command to be executed as the action.
		Automated action definition file (`actdef.conf`) (for conversion)	Defines (for conversion) conditions for executing an automated action and the command to be executed as the action.
		Automatic action notification definition file (`actnotice.conf`)	Defines the automated action status notification function.
		Extended startup process definition file (`jp1co_service.conf`)	Defines process information for the functions that constitute JP1/IM - Manager.
		IM parameter definition file (`jp1co_param_V7.conf`)	Defines whether a JP1 event is to be issued when JP1/IM - Manager processes fail or when JP1/IM - Manager processes are recovered automatically from abnormal termination.
		System profile (`.system`)	Defines environment information for the basic operation of the event console.
		User profile (`defaultUser` | `profile_`*user-name*)	Defines environment information for how the Event Console window is displayed.
		Communication environment definition file (`console.conf.update`)	Defines communication processing (timeout period) among JP1/IM - Manager, the viewer, and the `jcochstat` command.
		Health check definition file (`jcohc.conf`)#3	Defines whether the health check function is to be enabled.
		Event guide information file (`jco_guide.txt`)#3,#4	Defines event guide information for JP1 events that occur in the system and create problems.
		Event guide information sample file (`sample_jco_guide_ja.txt`, `sample_jco_guide_en.txt`)#3	Sample files that defines event guide information for JP1 events that occur in the system and create problems.
		Status event definition file (`processupdate.conf`)	Defines whether a JP1 event is to be issued when the action status changes.

Product name		Definition file name	Description
		Correlation event generation system profile (egs_system.conf)[#3]	Defines the start and stop operations for the Event Generation Service.
		Correlation event generation definition file[#3,#4]	Defines the JP1 event conditions that result in generation of correlation events and the correlation events that are generated when the JP1 event conditions are satisfied.
		Correlation event generation environment definition file[#3,#4]	Defines the size and number of correlation event generation history files.
		Definition file for manually registering incidents (incident.conf)	A definition file for linkage with JP1/Service Support. The file defines JP1/Service Support for linkage with JP1/IM - View.
		Configuration file for incident inheritance information(incident_info.conf)	A configuration file for linkage with JP1/Service Support. The file defines JP1 events' attributes and character strings to be inherited by incidents.
		Severity changing definition file (jcochsev.conf)[#3]	Defines conditions for changing the severity of JP1events and the new severity level.
		Command button definition file (cmdbtn.conf)[#3]	Defines command buttons to be displayed in the Execute Command window.
		File that defines which items are displayed for event conditions (attr_list.conf)	Specifies the conversion rules for the automated action and command execution event inheritance function.
		Configuration file for converting information (event_info_replace.conf)	Specifies the conversion rules for the automated action event inheriting function.
		Item file	Specifies the JP1 event attributes that are to be output during output of event reports.
		Environment definition file for event report output (evtreport.conf)	Defines the execution environment of the event report output function.
		Filter file	Defines filter conditions to be applied during output of event reports.
		System color definition file (systemColor.conf)[#3]	Defines the color settings used for an event list.
		Definition file for extended event attributes[#3,#4]	Defines extended attributes of JP1 events.
		Definition file for extended event attributes (extended file)[#3,#4]	Defines the settings for displaying program-specific extended attributes of JP1 events as item names on the screen and in the output of event reports.
		Definition file for object types	Defines the object types of the extended attributes of JP1 events.
		Common-exclusion-conditions extended definition file[#3,#4]	Defines the event conditions or the applicable period of the extended-mode common exclusion-conditions.
		Common-exclusion-conditions display item definition file (common_exclude_filter_attr_list.conf)[#3]	Specifies the items to be displayed in the **Attribute name** display area in the Common Exclusion-Conditions Settings (Extended) window.

Product name		Definition file name	Description
		Common-exclusion-conditions auto-input definition file (`common_exclude_filter_auto_list.conf`)#3	Defines JP1 event attributes that are set automatically when the Common Exclusion-Conditions Settings (Extended) window opens.
		Display item definition file for the repeated event condition (`event_storm_attr_list.conf`)#3	Specifies the items to be displayed in the **Attribute name** display area in the Repeated Event Condition Settings window.
		Auto-input definition file for the repeated event condition (`event_storm_auto_list.conf`)#3	Defines the attribute of a JP1 event that is set automatically when the Repeated Event Condition Settings window opens.
		Display item definition file for the severity change definition (`chsev_attr_list.conf`)#3	A definition file that specifies the items to display in the **Attribute name** display area of the Severity Change Definition Settings window.
		Auto-input definition file for the severity change definition (`chsev_auto_list.conf`)#3	Defines the JP1 event attribute that is set automatically when the Severity Change Definition Settings window opens.
		Definition file for opening monitor windows#3,#4	Defines settings for opening monitor windows.
		Email environment definition file (`jimmail.conf`)	A definition file that sets information necessary to send an email by using JP1/IM - Manager.
		Display message change definition file (`jcochmsg.conf`)#3	Defines the JP1 event conditions and new messages when changing the display of messages using the event display message change function.
		Display item definition file for a display message change definition (`chmsg_attr_list.conf`)#3	Specifies the items to be displayed in the **Attribute name** display area of the Display Message Change Definition Settings window.
		Automatic input definition file for a display message change definition (`chmsg_auto_list.conf`)#3	Specifies the conditions to be automatically set when the Display Message Change Definition Settings window opens.
		Environment definition file for events after the display message is changed (`chmsgevent.conf`)	Defines the behavior of the function for issuing an event when a display message is changed.
	Central Scope	Host information file (`jcs_hosts`)	Defines the host information that is managed by JP1/IM - Manager (Central Scope).
		Guide information file (`jcs_guide.txt`)#1	Defines guide information about the JP1 events that trigger a change in monitoring object status.
		Settings file for the maximum number of status change events (`evhist_warn_event_`*`xxx`*`.conf`)#2	Defines whether a JP1 event is to be issued when the number of status change events for a monitoring object exceeds a maximum value.
		Settings file for the completed-action linkage function (`action_complete_`*`xxx`*`.conf`)#2	Defines whether the completed-action linkage function is to be enabled.
		Definition file for automatic delete mode of status change event	Defines whether the function that automatically deletes the status change events when a JP1 event's status becomes `Processed` is to be enabled.
		Definition file for monitoring object initialization mode	Defines whether the function that initializes monitoring objects when a specific JP1 event is received is to be enabled.

Product name		Definition file name	Description
		Automatic backup and recovery settings file for the monitoring object database (auto_dbbackup_*xxx*.conf)[#2]	Defines whether the function that protects the monitoring object database from corruption caused by OS shutdown or cluster system switching during monitoring tree update processing is to be enabled.
		Definition file for on memory mode of status change condition	Specifies whether the memory-resident status change condition function is to be enabled.
		System profile of Central Scope (jcs_sysprofile_*xxx*.def)[#1]	Common definition information for Central Scope viewer. When you log in to Central Scope, this file is sent to Central Scope viewer.
	IM Configuration Management	Operation definition file for IM Configuration Management - View (jcfview.conf)	Specifies the operation of IM Configuration Management - View.
		Apply-IM-configuration-method definition file (jp1cf_applyconfig.conf)	Defines how to apply the system hierarchy.
		Host input information file (host_input_data.csv)	An export file for host input information related to managed hosts of IM Configuration Management.
		Collected host information file (host_collect_data.csv)	An export file for collected host information related to managed hosts of IM Configuration Management.
		Profile management environment definition file (jp1cf_profile_manager.conf)	Defines information about the execution environment for the profile management function.
		Remote log trap environment definition file (jp1cf_remote_logtrap.conf)	Defines the execution environment for the remote-monitoring log file trap function and the remote-monitoring event log trap function.
		Remote-monitoring log file-trap action definition file	Defines actions for the remote monitoring log trap function.
		Remote-monitoring event log trap action-definition file	Defines actions for the remote monitoring event log trapping function.
	IM database	Setup information file (jimdbsetupinfo.conf)	Specifies setup information, such as the size of the IM database and the directory for storing data for the IM database, when the integrated monitoring database and IM Configuration Management database are set up.
		Cluster setup information file (jimdbclustersetupinfo.conf)	A file that describes the directory to store the size or data of the IM database for a logical host when the integrated monitoring database and IM Configuration Management database are set up in a cluster environment.
	Intelligent Integrated Management Database	Intelligent Integrated Management Database setup information file (jimgndbsetupinfo.conf)	File that describes the items required when setting up Intelligent Integrated Management Database.
		Cluster environment Intelligent Integrated Management Database setup information file (jimgndbclustersetupinfo.conf)	A File that describes the items required when setting up a clustered Intelligent Integrated Management Database environment.
		Intelligent Integrated Management Database configuration file (postgresql.conf)	File that describes the parameter definition for Intelligent Integrated Management Database (PostgreSQL).

Product name		Definition file name	Description
	Product plug-ins of JP1/IM - Agent	Node exporter metric definition file (metrics_node_exporter.conf)#3	This File defines metric of Node exporter to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		Process exporter metric definition file (metrics_process_exporter.conf)#3	This file defines Process exporter metric information shown in the **Trends** tab of the Integrated Operation Viewer window.
		Node exporter (Service monitoring) metric definition file (metrics_node_exporter_service.conf) #3	This file defines metric information of Node exporter (Service monitoring) displayed on the [Trend] tab of [Integrated Operation Viewer] window.
		Windows exporter metric definition file (metrics_windows_exporter.conf)#3	This File defines metric of Windows exporter to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		Windows exporter (process monitoring) metric definition file (metrics_windows_exporter_process.conf)#3	This file defines Windows exporter (process monitoring) metric information shown in the **Trends** tab of the Integrated Operation Viewer window.
		Windows exporter (Service monitoring) metric definition file (metrics_windows_exporter_service.conf) #3	This file defines metric information of Windows exporter (Service monitoring) displayed on the [Trend] tab of [Integrated Operation Viewer] window.
		Node exporter for AIX metric definition file (metrics_node_exporter_aix.conf) #3	This file defines metric information of Node exporter for AIX displayed on the [Trend] tab of [Integrated Operation Viewer] window.
		Blackbox exporter metric definition file (metrics_blackbox_exporter.conf)#3	This File defines metric of Blackbox exporter to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf)#3	This File defines metric of Yet another cloudwatch exporter to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		Promitor metric definition file (metrics_promitor.conf)#3	This file defines Promitor metric information shown in the **Trends** tab of the Integrated Operation Viewer window.
		Script exporter metric definition file (metrics_script_exporter.conf)#3	This file defines Script exporter metric information shown in the **Trends** tab of the Integrated Operation Viewer window.
		Fluentd metric definition file (metrics_fluentd.conf)#3	This File defines metric of Fluentd to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		OracleDB exporter metric definition file (metrics_oracledb_exporter.conf) #3	This file defines metric information of OracleDB exporter displayed on the [Trend] tab of [Integrated Operation Viewer] window.
		OracleDB exporter default collection metric definition file (default-metrics.toml)	A file that defines the metrics that the OracleDB exporter retrieves.
		Container monitoring metric definition file (metrics_kubernetes.conf)#3	This file defines the container monitoring metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Product name		Definition file name	Description
		Any Prometheus trend name metric definition file (metrics_*any-Prometheus-trend-name*.conf)[#3,#4]	This File defines metric to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.
		User-specific metric definition file (metrics_*any-Prometheus-trend-name*.conf)[#3,#4]	A File that defines your own metric properties to be displayed on the [Trends] tabbed page of Integrated Operation Viewer window.
		User-specific metric definition file (Promitor) (metrics_*any-Prometheus-trend-name*.conf)[#3,#4]	This file defines the user specific metric information which displayed in the Trend tab of Integration Operation Viewer window.
		User-specific metric definition file (container monitoring) (metrics_*any-Prometheus-trend-name*.conf)[#3,#4]	This file defines the user specific metric information which displayed in the Trend tab of Integration Operation Viewer window.
		AWS definition file (aws_settings.conf)[#3]	Configuration file for AWS and Yet another cloudwatch exporter.
	JP1/IM - Agent (JP1/IM agent management base)	imbase common configuration file (jpc_imbasecommon.json)	This configuration file defines Common operation of JP1/IM agent management base.
		imbase configuration file (jpc_imbase.json)	This configuration file defines the operation of imbase process in JP1/IM agent management base.
		imbaseproxy configuration file (jpc_imbaseproxy.json)	This configuration file defines the operation of imbaseproxy process in JP1/IM agent management base.
JP1/IM - View		Communication environment definition file (view.conf.update)	Defines timeout periods for communication between JP1/IM - View and JP1/IM - Manager (Central Console).
		Communication environment definition file (tree_view.conf.update)	Defines timeout periods for communication between JP1/IM - View and JP1/IM - Manager (Central Scope).
		Non-encryption communication host configuration file (nosslhost.conf)	Configures hosts that use non-encrypted communication.
		IM-View settings file (tuning.conf)	Defines the operation of JP1/IM - View, such as the number of connected-host log entries in the Login window and the operation when the Event Console window is displayed.
		Web page call definition file (hitachi_jp1_*product-name*.html)	Used for calling another product's Web page from the Tool Launcher window.
		Start program definition file (!JP1_CS_APP0.conf)	Defines the start path for a program that is added to the toolbar in the Monitoring Tree window.
		Toolbar definition file (!JP1_CS_FTOOL0.conf)	Defines the order of programs that are added to the toolbar in the Monitoring Tree window.
		Icon operation definition file (!JP1_CS_FTREE0.conf)	Defines the operation of icons that are added to the toolbar in the Monitoring Tree window.
		Configuration file for monitoring tree	Defines the configuration of the monitoring tree that is displayed in the Monitoring Tree window.
		Definition file for executing applications	Defines the IDs and paths of applications that are executed by the viewer.

Product name	Definition file name	Description
	Definition file for the Tool Launcher window	Defines the tree that is to be displayed in the Tool Launcher window.
	System profile of the Central Scope viewer (system.conf)	Central Scope Viewer common definition information. Defines the Monitoring Tree (Editing) window and the Visual Monitoring (Editing) window.
	Performance report display definition file (performance.conf)	Defines the function for displaying the performance report of the host that issued the event. This file defines the URL of the connection-target instance of JP1/PFM - Web Console.
JP1/IM - Agent	Alertmanager configuration file (jpc_alertmanager.yml)#3	A configuration file that defines the operation of Alertmanager.
	Prometheus configuration file (jpc_prometheus_server.yml)#3	A configuration file that defines the operation of Prometheus server.
	Alert configuration file (jpc_alerting_rules.yml)#3	A File that defines the alert-evaluation rules that Prometheus server will Execute.
	Node exporter discovery configuration file (jpc_file_sd_config_node.yml)#3	A File that Setup Node exporter that Prometheus server will scrape.
	Process exporter discovery configuration file (jpc_file_sd_config_process.yml)#3	This file configures the Process exporter to be scraped by the Prometheus server.
	Windows exporter discovery configuration file (jpc_file_sd_config_windows.yml)#3	A File that Setup Windows exporter that Prometheus server will scrape.
	Node exporter for AIX discovery configuration file (jpc_file_sd_config_node_aix.yml)#3	Files that set Node exporter for AIX that Prometheus server will scrape.
	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file (jpc_file_sd_config_blackbox_http.yml)#3,#5	A File that Setup Blackbox exporter that Prometheus server will scrape for HTTP/HTTPS monitoring.
	Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file (user-created) (file_sd_config_blackbox_*module-name-start-with-http*.yml) #3,#5	
	Blackbox exporter (ICMP monitoring) discovery configuration file (jpc_file_sd_config_blackbox_icmp.yml)#3	A File that Setup Blackbox exporter that Prometheus server will scrape for ICMP monitoring.
	Blackbox exporter (ICMP monitoring) discovery configuration file (user-created) (file_sd_config_blackbox_*module-name-start-with-icmp*.yml)#3,#5	
	Yet another cloudwatch exporter discovery configuration file (jpc_file_sd_config_cloudwatch.yml)#3,#5	A File that Setup Yet another cloudwatch exporter that Prometheus server will scrape.
	Promitor discovery configuration file (jpc_file_sd_config_promitor.yml)#3	This file configures the Promitor to be scraped by the Prometheus server.

Product name	Definition file name	Description
	OracleDB exporter discovery configuration file (jpc_file_sd_config_oracledb.yml)#3	Files that set OracleDB exporter that Prometheus server will scrape.
	Script exporter discovery configuration file (jpc_file_sd_config_script.yml)#3	This file configures the Script exporter to be scraped by the Prometheus server.
	User-specific discovery configuration file (user_file_sd_config_*any-name*.yml)#3,#5	A File that Setup Prometheus server to scrape. Exporter that you have prepared can also be subject to scrape.
	Service definition file (jpc_*program-name*_service.xml)	A WinSW definition File for make programs Windows-service in a Windows environment.
	Unit definition file (jpc_*program-name*.service)	A definition File for add programs to systemctl Add in a Linux.
	Windows exporter configuration file (jpc_windows_exporter.yml)#3	A configuration file that defines the operation of Windows exporter.
	Process exporter configuration file (jpc_process_exporter.yml)#3	The configuration file that determines the behavior of Process exporter.
	Blackbox exporter configuration file (jpc_blackbox_exporter.yml)#3	A configuration file that defines the operation of Blackbox exporter.
	Yet another cloudwatch exporter configuration file (jpc_ya_cloudwatch_exporter.yml)#3	A configuration file that defines the operation of Yet another cloudwatch exporter.
	Promitor Scraper configuration file (metrics-declaration.yaml)#3	The configuration file that defines the metrics to be acquired by the Promitor Scraper.
	Promitor Scraper runtime configuration file (runtime.yaml)#3	The configuration file that defines Promitor Scraper authentication information, ports used for scraping, and other information.
	Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml)#3	The configuration file that defines the resource group to be acquired by Promitor Resource Discovery.
	Promitor Resource Discovery runtime configuration file (runtime.yaml)#3	The configuration file that defines Promitor Resource Discovery authentication information, ports used for scraping, and other information.
	Script exporter configuration file (jpc_script_exporter.yml)#3	The configuration file that determines the behavior of Script exporter.
	Sample file of Script exporter configuration file for SAP system monitoring (jpc_script_exporter_sap.yml)	This is a sample file of a configuration file that defines the operation of the Script Exporter for SAP system monitoring.
	Log monitoring common definition file (jpc_fluentd_common.conf)#3	A File for defining Common behavior in fluentd, such as HTTP POST request function and log output function.
	Log monitoring target definition file (jpc_fluentd_common_list.conf)#3	A File that specifies what to monitor for logging. Specifies File of monitoring definition file, which is text-formatted log file, or Windows event-monitoring definition file. The logging monitoring of the specified definition File is set to Enable.

Product name	Definition file name	Description
	Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)[#3,#5]	A Definition File for monitoring text-formatted log File.
	Windows event log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)[#3,#5]	A Definition File for monitoring Windows event logs.
	Sample file of system log information monitoring definition file for SAP system (fluentd_sap_syslog_tail.conf)	Sample file of the definition file for monitoring system log information of SAP system.
	Sample file of CCMS alert information monitoring definition file for SAP system (fluentd_sap_alertlog_tail.conf)	Sample file of the definition file used to monitor CCMS alerting for SAP system.
	Environment parameters file for jr3slget command (jr3slget.ini)	This file is used to set the output destination file name of the system log information of SAP system.
	Sample file of environment parameters file for jr3slget command (jr3slget.ini.sample)	This file is used to set the output destination file name of the system log information of SAP system.
	Environment parameters file for jr3alget command (jr3alget.ini)	This file is used to set the output-destination filename of CCMS alert information of SAP system.
	Sample file of environment parameters file for jr3alget command (jr3alget.ini.sample)	This is a sample file of a file that sets the output destination file name of the CCMS alert information of the SAP system.
	Log metrics definition file (fluentd_*any-name*_logmetrics.conf)[#3#5]	The Fluentd metric definition file used to read logs output by the application being monitored and convert them into log metrics.
	Property label definition file (property_labels.conf)	The definition file used to convert IM management node property values into separate values.
	imagent common configuration file (jpc_imagentcommon.json)	A configuration file defines Common operation of JP1/IM agent control base.
	imagent configuration file (jpc_imagent.json)	A configuration file defines imagent operation of JP1/IM agent control base.
	imagentproxy configuration file (jpc_imagentproxy.json)	A configuration file defines imagentproxy operation of JP1/IM agent control base.
	imagentaction configuration file (jpc_imagentaction.json)	A configuration file defines imagentaction operation of JP1/IM agent control base.
	User-created definition file list definition file (jpc_user_deffile_list.json)[#3]	A File that defines a user-created File that can be updated and delete with JP1/IM - Manager supplied REST API.
	Definition file property file (jpc_file_properties.json)	A File describes File name, File path, and File import operations for the definition File that are to be manipulated by the acquisition or update functions of the definition File.
	Environment variable file (any file name)[#3,#5]	A File that defines an environment-variable for Execute commands on JP1/IM managed hosts.

#1: The file name of the guide information file used in the system profile of Central Scope, and UNIX version of JP1/IM - Manager depend on the language used by the JP1/IM - Manager. The *xxx* part of the guide information file is explained later in the section describing details of each file.

#2: There are two settings files for the maximum number of status change events, two settings files for the completed-action linkage function, and two automatic backup and recovery settings files for the monitoring object database. Either `on` or `off` is set in *xxx*.

#3: A definition File that you can update using integrated operation viewer (for downloading and uploading a definition File) or REST API (for acquiring and updating a definition File). The following File can also be updated:

- File for Blackbox exporter
  CA certificate File, client certificate File, client certificate key File, Password File

#4: Definition File that can be specified in *User-created definition file list definition file (imdd_user_deffile_list.json)*.

#5: Definition File that can be specified in *User-created definition file list definition file (jpc_user_deffile_list.json)*. You can also specify the following File:

- File for Blackbox exporter
  CA certificate File, client certificate File, client certificate key File, Password File

Format of definition file explanations

This section describes the format of the definition file. Note that some of the items shown below might be omitted in some definition file explanations. Do not use any environment-dependent character in definition files or definition file names. Such a character might cause character corruption.

Format

Describes the format of the definition file.

File

Shows the name of the definition file.

Storage directory

Describes the definition file's storage location.

Description

Describes the use of the definition file.

When the definitions are applied

Describes when the definition file's contents are applied.

Information that is specified

Describes the information that is specified in the definition file.

Example definition

Provides an example of the definition file.

Definition files for displaying user-specific event attributes

You can extend the functions for linking JP1/IM to other applications by customizing JP1/IM definition files.

Customizing JP1/IM definition files

Extending functions enables you to do the following:

- Display user-specific event attributes
- Display the monitor window from JP1 events displayed in JP1/IM - View
- Add new menus to the Tool Launcher window

Note:

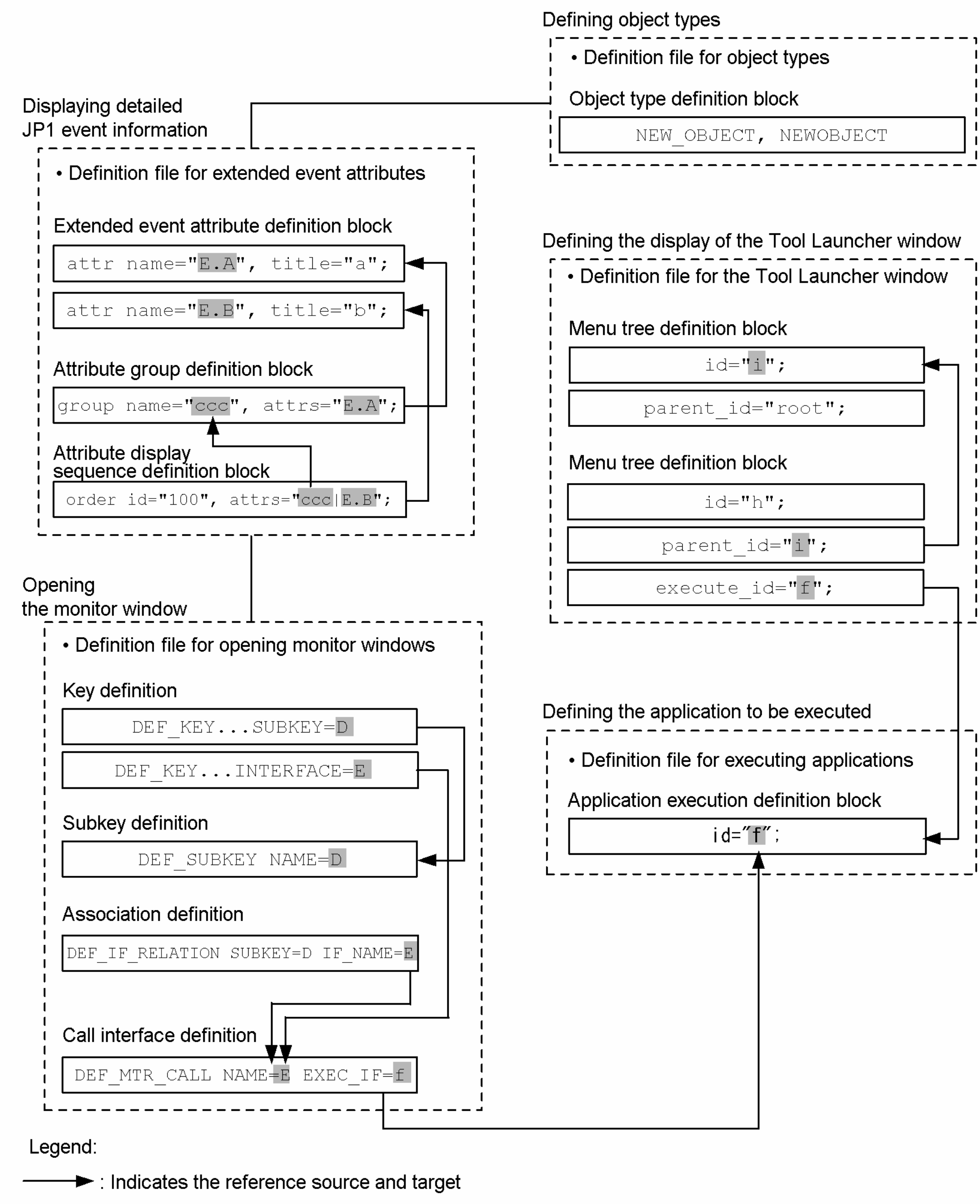
If you use UTF-8 as the encoding to save a customized definition file, save the file without attaching a BOM (byte order mark).

For details about the functions, see *4.14 Displaying user-defined event attributes* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Overview of definition files

In a definition file, blocks that specify definitions are related to each other. Moreover, the definition files are related to each other. The following figure shows these relationships.

Figure 2–1: Relationships between definition blocks and definition files


Defining object types
• Definition file for object types
Object type definition block
NEW_OBJECT, NEWOBJECT
Displaying detailed JP1 event information
• Definition file for extended event attributes
Extended event attribute definition block
attr name="E.A", title="a";
attr name="E.B", title="b";
Attribute group definition block
group name="ccc", attrs="E.A";
Attribute display sequence definition block
order id="100", attrs="ccc|E.B";
Defining the display of the Tool Launcher window
• Definition file for the Tool Launcher window
Menu tree definition block
id="i";
parent_id="root";
Menu tree definition block
id="h";
parent_id="i";
execute_id="f";
Opening the monitor window
• Definition file for opening monitor windows
Key definition
DEF_KEY...SUBKEY=D
DEF_KEY...INTERFACE=E
Subkey definition
DEF_SUBKEY NAME=D
Association definition
DEF_IF_RELATION SUBKEY=D IF_NAME=E
Call interface definition
DEF_MTR_CALL NAME=E EXEC_IF=f
Defining the application to be executed
• Definition file for executing applications
Application execution definition block
id="f";
Legend:
: Indicates the reference source and target

Naming rules for definition files

The following shows the naming rules for definition files.

Table 2–2: Naming rules for definition files

Definition file	Naming rule
Definition file for extended event attributes	*company-name_product-name*`_attr_en.conf`
Definition file for object types	*company-name_product-name*`_obj.en`
Definition file for executing applications	*company-name_product-name*`_app.conf`
Definition file for opening monitor windows	*company-name_product-name*`_mon.conf`
Definition file for the Tool Launcher window	*company-name_product-name*`_tree.conf`

Note that *product-name* may also be specified as *series-name_product-name*. We recommend that for JP1 event issuance you use as the file name the value specified in `PRODUCT_NAME`, with the forward slash (`/`) replaced by the underscore (_). Because `hitachi` is used as the default file name, use a name other than `hitachi` for *company-name*.

Storage locations for definition files

The following shows the storage location for each definition file.

Table 2–3: Storage locations for definition files

Definition file	Storage location
Definition file for extended event attributes	Machine where JP1/IM - Manager is installed
Definition file for opening monitor windows	Machine where JP1/IM - Manager is installed
Definition file for object types	Machine where JP1/IM - Manager is installed
Definition file for executing applications	Machine where JP1/IM - View is installed
Definition file for the Tool Launcher window	Machine where JP1/IM - View is installed

Structures of definition files

This section provides information that is common to the JP1/IM definition files that can be customized in order to link with the Event Console window and Tool Launcher window.

The information provided in this section is applicable to the following three definition files:

- Definition file for extended event attributes
- Definition file for executing applications
- Definition file for the Tool Launcher window

The definition file for object types and the definition file for opening monitor windows have different structures.

Components of definition files

The principal components of a definition file are the statement, blocks, and comments. A definition file begins with the statement that represents the attributes of the entire file (definition information header), followed by blocks that describe the details of the definition and any comments.

The following describes these components of a definition file.

Statement

Structure of a statement

A statement consists of multiple components that form a single meaning. A statement always begins at the beginning of a line and ends with a semicolon (`;`), followed by a linefeed code.

Types of statements

Statements are classified as in-file statements and in-block statements.

In-file statements

An in-file statement indicates attributes of the definition file. There are two types of in-file statements: statements for the definition information header, and statements for block control. Each statement in a file is prefixed with `@`.

In-block statements

An in-block statement indicates attributes of a block. All statements that can be specified between the start-of-block statement (`@define-block`) and the end-of-block statement (`@define-block-end`) are in-block statements, except for comments. The in-block statements that can be specified depend on the block.

In-block statements are not prefixed (i.e., there is no `@`).

Block

Structure of a block

A block consists of a set of statements. The set of statements includes a statement that declares the start of the block (`@define-block`), statements within the block that describe the actual definitions, comments, and a statement that declares the end of the block (`@define-block-end`).

Nested blocks are not allowed in a definition file.

Block type

A block's type is specified in the `type=` parameter of the start-of-block statement (`@define-block`). For details about the types of blocks, see *@define-block statement*.

Block priority

A block contains a key item that must be unique within the definition. If the definition contains multiple key items, one of the blocks is selected according to a priority ranking. The block priorities are as follows:

1. Block in the last file when file names are sorted in ascending order
2. Last block specified in the file

In other words, when definition files are linked into a single file in ascending order of the file names, the last block in the linked file has priority.

Comment

A comment is a line beginning with a hash mark (`#`) or a line consisting of only spaces, tabs, or a linefeed code. Comments do not contain definition information.

A comment is processed as a single statement. Because comments are evaluated by line, there is no need to delineate comments with a semicolon (`;`). If a comment ends with a semicolon (`;`), the semicolon is treated as part of the comment.

Rules for generating common Statements

The two types of in-file statements are statements for the definition information header and statements for block control.

The following table lists and describes the in-file statements.

Table 2–4: List of in-file statements

Statement name	Description	Type
`@file`	Declares the definition version.	For the definition information header
`@product`	Declares program product information in the definition.	For the definition information header
`@define-block`	Declares the beginning of a block.	For block control
`@define-block-end`	Declares the end of a block.	For block control

In these statements, a statement for the definition information header defines attributes that are common to the entire definition file. The available statements for the definition information header depend on the definition file. The parameters for the statements for the definition information header also depend on the definition file.

A statement for block control is used to declare a block unit that is defined in the definition file. The rules for generating statements for block control are common to all definition files. These rules are described below.

For the rules for generating statements for the definition information header, see the descriptions of the individual definition files.

@define-block statement

Syntax

`@define-block type="`*block-type*`";`

Function

Declares the beginning of a block. Statements from this statement to the `@define-block-end` statement are treated as a single definition block.

Parameter

`type="`*block-type*`"`

Specifies the type of definition block. The following lists the block types that can be specified.

Table 2–5: List of block types

Block name	Value in the parameter
Event attribute definition block	`"event-attr-def"`
Event attribute group definition block	`"event-attr-group-def"`
Event display sequence definition block	`"event-attr-order-def"`
Application execution definition block	`"application-execution-def"`
Menu tree definition block	`"function-tree-def"`

If an invalid block type is specified, the entire block is ignored and a warning is displayed, but file analysis processing continues.

Note:

Nested definition blocks are not allowed.

Example definition

See the description of the `@define-block-end` statement.

@define-block-end statement

Syntax

`@define-block-end;`

Function

Declares the end of a definition block that begins with `@define-block`.

Note:

If there is no corresponding `@define-block` statement, file analysis processing is canceled.

Example definition

This example includes `@define-block` and `@define-block-end` statements:

```
@define-block type="event-attr-def";
block lang="English", platform="base", extended="false";
attr name="E.SEVERITY", title="Severity";
attr name="B.TIME", title="Registered time";
attr name="B.SOURCESERVER", title="Registration host";
attr name="E.USER_NAME", title="User name";
@define-block-end;
```

Common definition settings file (changing the attribute of JP1 events)

Format

```
[JP1_DEFAULT\JP1CONFIG]
"ATTR_EVENT_LOGTRAP_SOURCEHOST"=dword:{00000000 | 00000001}
```

File

Use any file.

`jp1im_jp1_event_attributes.conf.model` (model file for the common definition settings file (changing the attribute of JP1 events)

Storage directory

The storage directory of the model file for the common definition settings file (changing the attribute of JP1 events) is shown below. Copy the model file to create a new file, and give it any file name.

In Windows

Manager-path`\conf`

In UNIX

`/etc/opt/jp1imm/conf`

Description

This file sets information about the source attribute of an event log trap as common definition information.

When the definitions are applied

When the `jbssetcnf` command is executed, information about the common definition settings file (changing the attribute of JP1 events) is registered as common definition information. Thereafter, when JP1/IM - Manager is restarted, the setting for the common definition information takes effect. If the common definition is changed, JP1/IM - Manager must be restarted.

Information that is specified

The following rules apply to the common definition settings file (changing the attribute of JP1 events):

- If `# (0x23)` is specified at the beginning of a line, the line is treated as a comment line.
- Do not enter a space or a tab before or after an equal sign (=) or a comma (`,`), at the beginning of a line, or at the end of a line. If you do so, an error occurs when the `jbssetcnf` command is executed.
- A line containing only a linefeed is invalid.

`[JP1_DEFAULT\JP1CONFIG]`

Do not change this line.

`"ATTR_EVENT_LOGTRAP_SOURCEHOST"=dword:{00000000 | 00000001}`

Determines the JP1/Base event log trap to be monitored by JP1/IM - Manager, and the attribute to be mapped to the event source host name attribute of a JP1 event for a remote-monitoring event log trap.

Specify either `00000000` or `00000001`. The default value is `00000000`.

If `00000000` is specified, a computer name is mapped to the event source host name of the JP1 event (event ID = 3A71).

If `00000001` is specified, the event server name is mapped to the event source host name of the JP1 event (3A71). In addition, the attribute of the event source host name is added to the JP1 event (3A71) for the remote-monitoring event log trap, and the monitored host name is displayed as the source host name.

For details about the attributes to be mapped to the event source host name of the JP1 event (3A71) for JP1/Base event log traps, see *15.3.10(2)(b) Changing JP1 event attributes (Setting for JP1/IM - Manager)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details about the JP1 event (3A71) for the remote-monitoring event log trap, see *3.2.2(97) Details of event ID: 00003A71, or the event ID specified in the filter block of the remote-monitoring event log trap action-definition file*.

Operation log definition file (imm_operationlog.conf)

Format

```
[logical-host-name\JP1IMM\OPERATION]
"ENABLE"=dword:hexadecimal-number
"LOGFILEDIR"="output-destination"
"LOGSIZE"=dword:hexadecimal-number
"LOGFILENUM"=dword:hexadecimal-number
```

Files

`imm_operationlog.conf`

`imm_operationlog.conf.model` (model file for the operation log definition file)

Storage directory

In Windows

Manager-path`\conf`

In UNIX

`/etc/opt/jp1imm/conf`

Description

This file specifies the common definition contents used by the operation log output function. Specify whether to output data to the operation log, the output destination and size of the operation log file, and the maximum number of log files that can be saved.

When the definitions are applied

When the `jbssetcnf` command is executed, the settings in the operation log definition file (`imm_operationlog.conf`) are registered in the common definition information. After that, the settings in the common definition information take effect when JP1/IM - Manager is restarted. If you change the common definition, you must restart JP1/IM - Manager.

Information that is specified

`[`*logical-host-name*`\JP1IMM\OPERATION]`

This entry indicates the key name of JP1/IM - Manager environment settings.

For the physical host, specify `JP1_DEFAULT` for *logical-host-name*. For a logical host, specify its name for *logical-host-name*.

`"ENABLE"=dword:`*hexadecimal-number*

Specify (using a hexadecimal number) whether to enable operation log output. The system assumes the initial value if this item is not defined or if you specify a value other than the following:

- Initial value: `0x00000000`
- To disable operation log output, specify `0x00000000`.
- To enable operation log output, specify `0x00000001`.

`"LOGFILEDIR"="`*output-destination*`"`

Specify (in absolute path format) the output destination of the operation log file (`imm_operation.log`). The maximum length of the output destination is 217 bytes. Specify an existing write-enabled directory for the output destination. We recommend that for the operation log of a logical host, specify an output destination on the shared disk.

- Initial value
  In Windows: *Manager-path*`\log\operationlog`
  In UNIX: `/var/opt/jp1imm/log/operationlog`
- Output destination example for a logical host:
  In Windows: *shared-folder*`\JP1IMM\log\operationlog`
  In UNIX: *shared-directory*`/jp1imm/log/operationlog`

Network paths cannot be specified as the output destination.

If the execution environment is a Windows environment, the following character strings cannot be specified for the output destination:

- Character strings that contain colons (:), question marks (?), double quotation marks ("), left angle brackets (<), right angle brackets (>), or vertical bars (|)
- Any of the following character strings (not case sensitive):
  CON, PRN, AUX, NUL, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8,or LPT9

`"LOGSIZE"=dword:`*hexadecimal-number*

Specify (by using a hexadecimal number in megabytes) the size of the operation log file (`imm_operation.log`) by using a hexadecimal number. The system assumes the initial value if this item is not defined or if you specify a value outside the specifiable range.

- Initial value: `0x00000005` (5 MB)
- Specifiable range: `0x00000001` to `0x00000800` (1 MB to 2,048 MB)

`"LOGFILENUM"=dword:`*hexadecimal-number*

Specify (using a hexadecimal number) the maximum number of operation log files (`imm_operation.log`) that can be saved. The system assumes the initial value if this item is not defined or if you specify a value outside the specifiable range.

- Initial value: `0x0000000A` (10 files)
- Specifiable range: `0x00000001` to `0x00000010` (1 to 16 files)

Example definition

The following shows an example of the operation log definition file for setting the log file size to 5 MB and for setting the maximum number of files that can be saved to 10. Note that the definition example shown below applies when JP1/IM - Manager is installed on a physical host whose OS is UNIX.

```
[JP1_DEFAULT\JP1IMM\OPERATION]
"ENABLE"=dword:00000001
"LOGFILEDIR"="/var/opt/jp1imm/log/operationlog"
"LOGSIZE"=dword:00000005
"LOGFILENUM"=dword:0000000A
```

Intelligent Integrated Management Base definition file (imdd.properties)

Format

```
server.port=port-number
jp1.imdd.proxy.server[n].host=host-name-of-proxy-server[n]
jp1.imdd.proxy.server[n].port=port-number-of-proxy-server[n]
jp1.imdd.proxy.server[n].user=authentication-user-ID-of-proxy-server[n]
jp1.imdd.proxy.target[n].host=target-host[n]-of-REST-API-that-uses-proxy-ser
ver
jp1.imdd.proxy.target[n].serverHost=target-host-name[n]-of-destination-proxy
-server
jp1.imdd.gui.settings.contentViews.<custom UI Id>.title=title-displayed-on-c
ustom-UI-tab
jp1.imdd.gui.settings.contentViews.<custom UI Id>.url=path-to-html-file-disp
layed-in-user-defined-window-display-area
jp1.imdd.gui.settings.contentViews.<custom UI Id>.sid=tree-SID-of-IM-managem
ent-node-on-which-user-defined-windows-are-displayed
jp1.imdd.gui.settings.contentViews.<custom UI Id>.target=SID-of-IM-managemen
t-node-on-which-user-defined-windows-are-displayed
jp1.im.db.DEFAULT.portNo=port-number-used-by-IM-database
jp1.im.db.DEFAULT.logicalHostNum=number-used-by-IM-database-for-logical-host
-to-identify-logical-host
jp1.imdd.gui.settings.linkedUnit.impact.unKnownDisplay=whether-to-show/hide-
impact-unknown-icon
jp1.imdd.event.stormCompatible=Compatible-setting-of-the-repeated-event-view
ing-suppression-function
jp1.imdd.gui.settings.eventSearchCount=number-of-searches-in-event-acquisiti
on
jp1.imdd.authBasic=whether-to-enable/disable-Basic-authentication
jp1.imdd.jp1LoginForm=true|false
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.client-name=alias-name-of-th
e-client
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.client-id=client-ID-configur
ed-in-the-OpenID-provider
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.client-authentication-method
=basic|post
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.authorization-grant-type=aut
horization_code
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.redirect-uri=URI-of-the-redi
rection-URL
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.scope=scope-used-for-the-cli
ent
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.authorization-uri=URI-of-the
-authorization-URL
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.token-uri=URI-of-the-URL-fro
m-which-the-token-is-obtained
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.user-info-uri=URI-of-the-use
r-information-URL
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.userNameAttribute=attribute-
name
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.jwk-set-uri=URI-of-the-JSON-
Web-Key-(JWK)-Set-URL
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.issuer-uri=Issuer-Identifier
-of-the-OpenID-provider
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.logout-uri=logout-URI-of-the
-OpenID-provider
```

```
jp1.imdd.oidc.<key-name-of-the-OpenID-provider>.introspect-uri=token-informa
tion-acquisition-URI-of-the-OpenID-provider
jp1.imdd.simt.updateMode=reconfigure|change
```

Files

`imdd.properties`

`imdd.properties.model` (model file for the Intelligent Integrated Management Base definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-folder`/jp1imm/conf/imdd/`

Description

This file defines system settings for the Intelligent Integrated Management Base.

When the definitions are applied

The specified definitions take effect when JP1/IM - Manager starts.

Information that is specified

The following rules apply to the Intelligent Integrated Management Base definition file:

- If `#` (`0x23`) is specified at the beginning of a line, the line is treated as a comment line.
- Property names are case sensitive.
- The definition file must be saved in UTF-8 without BOM (byte order mark).
- If an invalid property is found, the system ignores the line to continue.
- We cannot guarantee the behavior when a property is set to an unacceptable value.

`server.port=`*port-number*

Specifies a port number on which the Intelligent Integrated Management Base will receive HTTP connections.

The specified port number must be unique across the system and across the host that is created during the setup.

Acceptable values are from `5001` to `65535`. The default value is `20703`.

`jp1.imdd.proxy.server[n].host=`*host-name-of-proxy-server[n]*

Specifies the host name of proxy server `[`*n*`]`.

The specified host name of the proxy server must be able to be resolved. If an invalid host name is specified, product plug-ins fail to execute APIs.

Use ASCII characters to specify it.

If you specify this property multiple times, use serial numbers starting from 0 for `[n]`.

`jp1.imdd.proxy.server[n].port=`*port-number-of-proxy-server[n]*

Specifies the port number of proxy server `[n]`.

Possible values are 1 to 65535. If the specified value is beyond the range of the possible values, the `KAJY52016-W` message is output and the proxy server `[n]` setting is disabled.

If you specify this property multiple times, use serial numbers starting from 0 for `[n]`.

`jp1.imdd.proxy.server[n].user=`*authentication-user-ID-of-proxy-server[n]*

Specifies the user ID of the authentication user for proxy server `[n]`.

If you use proxy server authentication, you must specify this option and configure authentication information for the proxy server. For details about the authentication information settings for the proxy server, see *jddsetproxyuser* in *Chapter 1. Commands*.

If you specify this property multiple times, use serial numbers starting from 0 for `[n]`.

If you do not use proxy server authentication, you can omit this option.

`jp1.imdd.proxy.target[n].host=`*target-host[n]-of-REST-API-that-uses-proxy-server*

Specifies the host for target `[n]` that is a target of REST API which uses the proxy server. The host name of target `[n]` must have the host section in the URL of the REST API.

For example, if the REST API has the http://hitachi.co.jp/api/v1/restApi value, specify `hitacih.co.jp`.

Use ASCII characters to specify it.

If you specify this property multiple times, use serial numbers starting from 0 for `[n]`.

`jp1.imdd.proxy.target[n].serverHost=`*target-host-name[n]-of-destination-proxy-server*

Specifies the host name of proxy server `[n]` working as the destination.

If the specified value is not configured for proxy server `[n]` or is invalid, the `KAJY52018-W` message is output and the settings for target host `[n]` are disabled.

Use ASCII characters to specify it.

If you specify this property multiple times, use serial numbers starting from 0 for `[n]`.

`jp1.imdd.gui.settings.contentViews.<custom UI Id>.title=`*title-displayed-on-custom-UI-tab*

Specifies the title displayed on the custom UI tab when the custom UI display function is used.

The title must be a string with 255 or fewer characters that contains neither control nor machine-dependent characters.

If you use multi-byte characters, convert them into Unicode format (which is expressed as `\u`*dddd*). In this case, the number of characters is counted as the number of them converted into Unicode.

You must specify this option for every `<custom UI Id>`.

`jp1.imdd.gui.settings.contentViews.<custom UI Id>.url=`*path-to-html-file-displayed-in-user-defined-window-display-area*

Specifies the path to the html file displayed in **User-defined window display area** in relative path format to `public` when the custom UI display function is used. The html file is located in the following location:

In Windows

Manager-path`\public\customUI\`

In UNIX

`/opt/jp1imm/public/customUI/`

Specify the path to the html file as a string with 255 or fewer characters that contains neither control nor machine-dependent characters. Use a forward slash (/) as a delimiter.

If you use multi-byte characters, convert them into Unicode format (which is expressed as \u*dddd*). In this case, the number of characters is counted as the number of them converted into Unicode. You do not have to enclose a space character ( ) with double quotation marks (").

You must specify this option for every <custom UI Id>.

`jp1.imdd.gui.settings.contentViews.<custom UI Id>.sid=`*tree-SID-of-IM-management-node-on-which-user-defined-windows-are-displayed*

Specifies the tree SID of the IM management node on which user-defined windows are displayed when the custom UI display function is used.

The tree SID of the IM management node you specify must have 1,048,576 or less characters. The characters allowed conform to the specifications of the tree SID specified.

You can use regular expressions when specifying the tree SID of an IM management node. The regular expressions work if they match perfectly. The condition will be true if the specified regular expression matches perfectly with the whole string of the tree SID of the IM management node after comparing the expression with the string. When regular expressions are used, it may take time for searching if `.*`, which matches any string, is used many times. If you want to use `.*`, do so only when it is really necessary.

Note that the system does not check whether the specified tree SID exists.

You must specify either `sid` or `target` for every `<custom UI Id>`.

`jp1.imdd.gui.settings.contentViews.<custom UI Id>.target=`*SID-of-IM-management-node-on-which-user-defined-windows-are-displayed*

Specifies the tree SID of the IM management node on which user-defined windows are displayed when the custom UI display function is used.

The tree SID of the IM management node you specify must have 1,048,576 or less characters. The characters allowed conform to the specifications of the tree SID specified. You can use regular expressions when specifying the SID of an IM management node. The regular expressions work if they match perfectly. The condition will be true if the specified regular expression matches perfectly with the whole string of the SID of the IM management node after comparing the expression with the string. When regular expressions are used, it may take time for searching if `.*`, which matches any string, is used many times. If you want to use `.*`, do so only when it is really necessary.

Note that the system does not check whether the specified tree SID exists.

You must specify either `sid` or `target` for every `<custom UI Id>`.

`jp1.im.db.DEFAULT.portNo=`*port-number-used-by-IM-database*

Specifies the port number used by the IM database.

For a physical host, use the value specified for the `IMDBPORT` option in the setup information file that is used during setup of the integrated monitoring database. If the `IMDBPORT` option is set to its default, you do not have to specify the `jp1.im.db.DEFAULT.portNo` value.

For details about the setup information file, see *Setup information file (jimdbsetupinfo.conf)*.

For a logical host, use the value specified for the `IMDBPORT` option in the cluster setup information file that is used during setup of the integrated monitoring database.

For details about the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)*.

`jp1.im.db.DEFAULT.logicalHostNum=`*number-used-by-IM-database-for-logical-host-to-identify-logical-host*

Specifies the number used by the IM database for a logical host to identify the host.

Specify the value used for the `LOGICALHOSTNUMBER` option in the cluster setup information file that is used during setup of the integrated monitoring database.

If a logical host is specified for `jp1.im.db.DEFAULT.portNo`, specify this option.

For details about the cluster setup information file, see *Cluster setup information file (jimdbclustersetupinfo.conf)*.

jp1.imdd.gui.settings.linkedUnit.impact.unKnownDisplay=*whether-to-show/hide-impact-unknown-icon*

Specifies whether to show an icon indicating that it is unknown whether there is any impact on following root jobnets (? icon) in the **Job flow** tab and the Linked unit dialog box.

Specify either `true` or `false`. Use `true` if you want to show the icon, or `false` if not. The default value is `true`.

`jp1.imdd.event.stormCompatible=`*Compatible-setting-of-the-repeated-event-viewing-suppression-function*

In version 12-00, repeated-event display is not suppressed even if the `-storm` option of the `jcoimdef` command is set to `ON`. Therefore, if you upgraded from version 12-00, to use the repeated event viewing suppression function, the compatible setting of the Repeated event viewing suppression function must be disabled (false).

If you new install a version 12-10 or later, the compatible setting of the repeated event viewing suppression Function is setting to Disabled (false) beforehand.

Specify either `true` or `false`.

If you set it to `true`, display of repeated events is not suppressed just like in 12-00. If you set it to `false`, display of repeated events is suppressed.

The default value is `true`.

The repeated-event display suppression function is enabled when suppression of repeated event monitoring in the `-storm` option of the `jcoimdef` command is set to `ON` and the `jp1.imdd.event.stormCompatible` option is set to `false`.

The repeated-event display suppression function is disabled when suppression of repeated event monitoring in the `-storm` option of the `jcoimdef` command is set to `OFF`, regardless of the `jp1.imdd.event.stormCompatible` option.

`jp1.imdd.gui.settings.eventSearchCount=`*number-of-searches-in-event-acquisition*

Specifies the number of searches during event acquisition that is performed by the integrated operation viewer to show the event list.

In event acquisition, the system searches for events mapped with the selected IM management node. Depending on the pages to be displayed, the search start position, search direction, and 100 events to be searched for are determined. If 100 events cannot be obtained due to an event receiver filter, the search is repeated for the next 100 events.

You specify the upper limit for the number of these repeated event searches. If the number of searches reaches the specified value, the search operation is interrupted and the events obtained before the interruption are displayed in the event list.

Possible values are 0 to 120000 (times). The number of times is unlimited if you specify `0` for it. The default is `10`. If a value beyond the possible values is specified, the default value is assumed for operation.

`jp1.imdd.authBasic=`*whether-to-enable/disable-Basic-authentication*

In any REST API of the Intelligent Integrated Management Base, you can use an authentication method with login information added to the REST API (Basic authentication). This option specifies whether to enable the Basic authentication.

Specify either `true` or `false`.

The Basic authentication is enabled if the option is set to `true`.

The default is `false`.

For details about the REST API, see *5. API*.

`jp1.imdd.jp1LoginForm=true|false`

Specifies whether the login form for JP1/Base authentication is displayed as the login window of the Intelligent Integrated Management Base.

When no OpenID provider is defined, the option assumes `true` for operation if it is set to `false`.

Furthermore, if it is set to `false` and only one OpenID provider is defined, the authentication URL of the OpenID provider is called directly without the use of the authentication window of the Intelligent Integrated Management Base.

Specify either `true` or `false`.

The JP1/Base authentication login form is enabled if the option is set to `true`.

The default is `true`.

`jp1.imdd.oidc.`*<key-name-of-the-OpenID-provider>*`.client-name=`*alias-name-of-the-client*

Specifies the alias name of the Intelligent Integrated Management Base client registered in the OpenID provider.

The alias name of the client is used as the name of the button on the login window of the Intelligent Integrated Management Base.

Specify a unique name with which the OpenID provider can be identified for *<key-name-of-the-OpenID-provider>*.

`jp1.imdd.oidc.`*<key-name-of-the-OpenID-provider>*`.client-id=`*client-ID-configured-in-the-OpenID-provider*

Specifies the ID of the Intelligent Integrated Management Base client registered in the OpenID provider.

Specify a unique name with which the OpenID provider can be identified for *<key-name-of-the-OpenID-provider>*.

`jp1.imdd.oidc.`*<key-name-of-the-OpenID-provider>*`.client-authentication-method=basic|post`

Specifies the authentication method used on the server that authorizes the Intelligent Integrated Management Base client registered in the OpenID provider.

Specify either `basic` or `post`.

The default is `basic`.

Specify a unique name with which the OpenID provider can be identified for *<key-name-of-the-OpenID-provider>*.

`jp1.imdd.oidc.`*<key-name-of-the-OpenID-provider>*`.authorization-grant-type=authorization_code`

Specifies the type of authorization granted to the Intelligent Integrated Management Base client registered in the OpenID provider.

Specify `authorization_code`.

Specify a unique name with which the OpenID provider can be identified for *<key-name-of-the-OpenID-provider>*.

`jp1.imdd.oidc.`*<key-name-of-the-OpenID-provider>*`.redirect-uri=`*URI-of-the-redirection-URL*

Specifies the URI of the redirection URL registered in the OpenID provider in the following format:

```
<Intelligent-Integrated-Management-Base-login-URI>/oauth2/code/<OpenID-pro
vider>
```

Example:

```
https://IMHOST:20703/login/oauth2/code/okta
```

Specify a unique name with which the OpenID provider can be identified for *<key-name-of-the-OpenID-provider>*. The permitted characters are a URL-formatted string. If the characters are specified in any other format, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

The authentication request is stored in the WWW browser and in the session of the Intelligent Integrated Management Base. Cookie data is managed on a domain basis. Therefore, make sure that the Intelligent Integrated Management server host name for the Intelligent Integrated Management Base login URI matches that for the URI of the redirection URL, and make sure that during authentication processing, the cookies are not removed or overwritten.

Also, if the Intelligent Integrated Management server host name for the Intelligent Integrated Management Base login URI and that for the URI of the redirection URL do not match, the `KAJY52028-E` message is output as a return value to the integrated operation viewer or REST API upon login by OpenID authentication.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.scope=`*scope-used-for-the-client*

Specifies the scope used for the Intelligent Integrated Management Base client registered in the OpenID provider. To specify multiple scopes, separate them with a comma (`,`).

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

The permitted characters are ASCII characters (0x21, 0x23 to 0x5B, and 0x5D to 0x7E). If any characters that are not permitted are specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.authorization-uri=`*URI-of-the-authorization-URL*

Specifies the URI of the authorization URL.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.token-uri=`*URI-of-the-URL-from-which-the-token-is-obtained*

Specifies the URI of the URL from which the token is obtained.

If a value that is not in the URL format is specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.user-info-uri=`*URI-of-the-user-information-URL*

Specifies the URI of the user information URL.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.userNameAttribute=`*attribute-name*

Specifies the name of the attribute used to access the name of the user based on the user information response.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.jwk-set-uri=`*URI-of-the-JSON-Web-Key-(JWK)-Set-URL*

Specifies the URI of the JSON Web Key (JWK) Set URL.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.issuer-uri=`*Issuer-Identifier-of-the-OpenID-provider*

Specifies the Issuer Identifier of the OpenID provider.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the `KAJY52019-W` message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

`jp1.imdd.oidc.`<*key-name-of-the-OpenID-provider*>`.logout-uri=`*logout-URI-of-the-OpenID-provider*

Specifies the logout URL of the OpenID provider.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the KAJY52019-W message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

jp1.imdd.oidc.<*key-name-of-the-OpenID-provider*>.introspect-uri=*token-information-acquisition-URI-of-the-OpenID-provider*

Specifies the token information acquisition URL of the OpenID provider.

Specify a unique name with which the OpenID provider can be identified for <*key-name-of-the-OpenID-provider*>.

If a value that is not in the URL format is specified, the KAJY52019-W message is output to disable the OpenID provider settings and the startup of the JP1/IM3-Manager service continues.

jp1.imdd.simt.updateMode=reconfigure|change

Specifies the default method for application when the jddupdatetree command is executed.

Specify either reconfigure or change.

If you specify reconfigure, the application is performed in the new and rebuilding mode, which is the same as version 12-10 or earlier. If you specify change, the application is performed in the configuration change mode.

The default value is change.

If this option is not defined, it assumes reconfigure. If an invalid value is specified, the option uses the default value, change.

Notes

When the Intelligent Integrated Management Base service starts, if this definition file does not exist or an attempt to read the file fails, the following behavior occurs.

For a physical host:

The KAJY00015-W message is output to the integrated trace log, the default value is tentatively set for the property, and the service starts.

For a logical host:

The KAJY00021-E message is output to the integrated trace log, and the Intelligent Integrated Management Base service ends.

Example definition

```
server.port=20703
jp1.imdd.proxy.server[0].host=ProxyServer
jp1.imdd.proxy.server[0].port=443
jp1.imdd.proxy.server[0].user=UserID
jp1.imdd.proxy.target[0].host=HostA
jp1.imdd.proxy.target[0].serverHost=ProxyServer

jp1.imdd.gui.settings.contentViews.sample.title=\u30ab\u30b9\u30bf\u30e0UI1
jp1.imdd.gui.settings.contentViews.sample.url=./customUI/sample/index.html
jp1.imdd.gui.settings.contentViews.sample.target=^(?=.*MYHOST).*$

jp1.imdd.gui.settings.contentViews.sample2.title=\u30ab\u30b9\u30bf\u30e0UI2
jp1.imdd.gui.settings.contentViews.sample2.url=./customUI/sample2/index.html
jp1.imdd.gui.settings.contentViews.sample2.sid=_ROOT_AllSystems

jp1.im.db.DEFAULT.portNo=20700
jp1.im.db.DEFAULT.logicalHostNum=[1-9]

jp1.imdd.gui.settings.linkedUnit.impact.unKnownDisplay=true
jp1.imdd.event.stormCompatible=false
```

```
jp1.imdd.gui.settings.eventSearchCount=10

jp1.imdd.authBasic=false

jp1.imdd.jp1LoginForm=true
jp1.imdd.oidc.keycloak.client-name=KEYCLOAK LOGIN
jp1.imdd.oidc.keycloak.client-id=jddmain
jp1.imdd.oidc.keycloak.client-authentication-method=basic
jp1.imdd.oidc.keycloak.authorization-grant-type=authorization_code
jp1.imdd.oidc.keycloak.redirect-uri=https://IMhost:20703/login/oauth2/code/keycloak
jp1.imdd.oidc.keycloak.scope=openid,profile,email,address,offline_access
jp1.imdd.oidc.keycloak.authorization-uri=https://OPhost:8080/auth/realms/jddmain/protocol/openid-connect/auth
jp1.imdd.oidc.keycloak.token-uri=https://OPhost:8080/auth/realms/jddmain/protocol/openid-connect/token
jp1.imdd.oidc.keycloak.user-info-uri=https://OPhost:8080/auth//realms/jddmain/protocol/openid-connect/userinfo
jp1.imdd.oidc.keycloak.userNameAttribute=sub
jp1.imdd.oidc.keycloak.jwk-set-uri=https://OPhost:8080/auth/realms/jddmain/protocol/openid-connect/certs
jp1.imdd.oidc.keycloak.issuer-uri=https://OPhost:8080/auth/realms/jddmain
jp1.imdd.oidc.keycloak.logout-uri=https://OPhost:8080/auth/realms/jddmain/protocol/openid-connect/logout
jp1.imdd.oidc.keycloak.introspect-uri=https://OPhost:8080/auth/realms/jddmain/protocol/openid-connect/token/introspect
jp1.imdd.simt.updateMode=change
```

System node definition file (imdd_systemnode.conf)

Format

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"first-system-name-ID",
      "displayName":"system-name-to-be-displayed",
      "jp1ResourcesGroup":"JP1-resource-group",
      "hostName":[{"host-name-string":"type"},...],
                   ...
                 ],
       "objectRoot":[
             {"type":"object-root-node-type",
              "name":[
                 {"object-root-node-string":"type"},
                    ...
                     ]
                    },
                    ...
             ],
      "children":[
        {
          "id":"first-subsystem-name-ID",
          "displayName":"subsystem-name-to-be-displayed",
          "jp1ResourcesGroup":"JP1-resource-group",
          "hostName":[
                       {"host-name-string":"type"},...],
                        ...
                     ],
            "objectRoot":[
                {"type":"object-root-node-type",
                 "name":[
                    {"object-root-node-string":"type"},
                       ...
                        ]
                       },
                       ...
                ],
          "children":[
            {
              "id":"subsystem-name-ID-under-second -subsystem",
              "displayName":"subsystem-name-to-be-displayed",
              "jp1ResourcesGroup":"JP1-resource-group",
              "hostName":[{"host-name-string":"type"},...],
              "objectRoot":[
                    {"type":"object-root-node-type",
                     "name":[
                        {"object-root-node-string":"type"},
                           ...
                            ]
                           },
                           ...
                    ]
              "children":[
                {
                  ...
                },
                ...
              ]
            },
            ...
          ]
        },
        {
          "id":"second-subsystem-name-ID",
          "displayName":"subsystem-name-to-be-displayed",
          "jp1ResourcesGroup":"JP1-resource-group",
          "hostName":[{"host-name-string"":"type"},...],
          "objectRoot":[
                {"type":"object-root-node-type",
                 "name":[
                    {"object-root-node-string":"type"},
                       ...
                        ]
                       },
                       ...
             ]
          "children":[
            {
              ...
            },
            ...
          ]
        },
        ...
      ]
    },
    {
      "id":"second-system-name-ID",
      ...
    },
    ...
  ]
}
```

Files

`imdd_systemnode.conf`

`imdd_systemnode.conf.model` (model file for the system node definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

This setting file defines the hierarchical structure of the system to represent it in a sunburst or tree chart, and sorts collected data into different groups of defined hosts or other object root nodes.

It defines in what system each host or other object root node in the configuration information collected by the Intelligent Integrated Management Base is located.

Displayed items include hosts and other object root nodes in the agent configuration or remote monitoring configuration of JP1/IM - Manager and any node contained in the configuration information collected from other products. If the AJS manager or PFM manager is included in the linking host of JP1/IM - Manager (Intelligent Integrated Management Base), child AJS agents and PFM monitoring agents are also displayed in the tree.

The list of hosts and other object root nodes is obtained when the `jddcreatetree` command is executed, and the hosts and other object root nodes are allocated under the system according to the system node definition file (`imdd_systemnode.conf`) to create the hierarchical structure. Therefore, even a host or other object root node defined in the system node definition file (`imdd_systemnode.conf`) is not displayed in the tree if it is not found in the configurations of JP1/IM, JP1/AJS, or JP1/PFM.

If one node is used in more than one system or subsystem, the host must be defined to be included in one of those systems. One node cannot be managed by more than one system.

When the definitions are applied

The settings in the system node definition file are applied to the Intelligent Integrated Management Base when the `jddcreatetree` and `jddupdatetree` commands are completed successfully.

For details about the `jddcreatetree` and `jddupdatetree` commands, see *jddcreatetree* and *jddupdatetree* in *Chapter 1. Commands*.

Information that is specified

The system node definition file must be saved in UTF-8 without BOM (byte order mark). If you specify a backslash (`\`) as part of a character string, immediately before `\`, specify `\` as an escape character.

`"version":"2"`

Specifies the version of the system node definition file. Set this to `2`. This option is mandatory.

`"id":"`*nth-system-name-(ID)*`"`

Specifies a system ID to be set in the SID (a unique ID representing a component of a linked product) with alphanumeric characters. `id` can be up to 255 characters in length. The total maximum number of systems and system components that you can specify is 1,000. This option is mandatory.

- For a system:
  The value must be unique across systems directly under `allSystem`.

- For a subsystem:

  The value must be unique across subsystems directly under `children`.

To merge the system node definition files due to system consolidation, check for the uniqueness of the identifiers and change the `id` values if necessary.

`"displayName":"`*system-name-to-be-displayed*`"`

Specifies the name of the system that will appear in a sunburst or tree chart.

The name can be up to 255 characters in length and must not include any control characters or machine-dependent characters. The value of `displayName` does not have to be unique in the system node definition file. It can be used multiple times.

`"jp1ResourcesGroup":"`*JP1-resource-group*`"`

Specifies a JP1 resource group to indicate an area to be monitored by the system. This field is not required unless you want to use JP1 resource groups to control access.

The value of `jp1ResourcesGroup` can be up to 64 characters in length and can include alphanumeric characters and the following symbols: exclamation mark (`!`), at mark (`@`), hash mark (`#`), dollar sign (`$`), percent sign (`%`), ampersand (`&`), underscore (_), hyphen (`-`), asterisk (`*`), single quotation mark (`'`), caret (`^`), left curly bracket (`{`), right curly bracket (`}`), left parenthesis (`(`), right parenthesis (`)`), period (`.`), backslash (`\`), grave accent mark (`` ` ``), and tilde (~).

`"hostName":[{"`*host-name-string*`":"`*type*`"}...]`

Specifies a list of hosts in the IM configuration and hosts that belong to the system, such as registration agents for linked products, with a combination of a host name string and type as follows.

Host name string	Type (6 or less characters)
Specify a host name directly	"" (Empty string)
Specify hosts using regular expressions#	`regexp`

# For the regular expression, use an extended regular expression. The regular expressions work if they match perfectly. The condition will be true if the specified regular expression matches perfectly with the whole string of the host name after comparing the expression with the string. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The host name can be up to 255 characters in length and can include alphanumeric characters and the following symbols: exclamation mark (`!`), dollar sign (`$`), left parenthesis (`(`), right parenthesis (`)`), asterisk (`*`), plus sign (+), comma (`,`), hyphen (`-`), period (`.`), forward slash (`/`), colon (`:`), left angle bracket (<), equal sign (=), left square bracket (`[`), backslash (`\`), right square bracket (`]`), caret (`^`), left curly bracket (`{`), vertical bar (`|`), and right curly bracket (`}`).

Example:

```
"hostName":[{"host1":""},{".+[1-5]+":"regexp"}]
```

The list of hosts specified in `hostName` is used to group data. The grouping proceeds from the top to the bottom of the list and handles host names case-insensitively. If a subsystem is not defined and `type` and `name` are not specified by `children`, this option cannot be omitted.

If duplicate host names are found, the second and further occurrences of the host name are ignored.

`"objectRoot"`

Specifies the object root node type, object root node string, and type of an object root node that belongs to a system or subsystem.

`"type":"`*object-root-node-type*`"`

Specifies the type of the object root node name specified as `name`.

The specified object root node type is not case sensitive. For details about values that can be specified for `type`, see the manual for each product. You can specify only the value of `HOST` when JP1/AJS or JP1/PFM is linked.

If a subsystem is not defined by `children` and `hostName` is not specified, this option cannot be omitted.

You can specify single-byte alphanumeric characters and symbols including hyphen (`-`), period (`.`), colon (`:`), and tilde (~) as `type`.

`"name":[{"`*object-root-node-string*`":"`*type*`"}...]`

Specifies the object root node string and type of an object root node that belongs to the system or a subsystem as follows.

Object root node string	Type
Specify an object root node string directly	"" (Empty string)
Specify hosts using regular expressions#	`regexp`

# For the regular expression, use an extended regular expression. The regular expressions work if they match perfectly. The condition will be true if the specified regular expression matches perfectly with the whole string of the object root node name after comparing the expression with the string. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Example 1:

```
"name":{"switch1":""}
```

Example 2:

```
"name":{".+[1-5]+":"regexp"}
```

The list of object root nodes specified in `name` is used to group data. The grouping proceeds from the top to the bottom of the list and handles object root nodes case-insensitively. If the object root node name specified for `name` and the object root node type specified for `type` are duplicated, the second and subsequent object root node names are ignored.

If a subsystem is not defined by `children` and `hostName` is not specified, this option cannot be omitted.

`"children"`

Specifies a list of subsystems that are directly under the system with the values of the fields from `id` to `children` to define a hierarchical structure. A hierarchical structure can have up to 10 levels including the top system. The `children` field is not required unless the system has subsystems directly under itself.

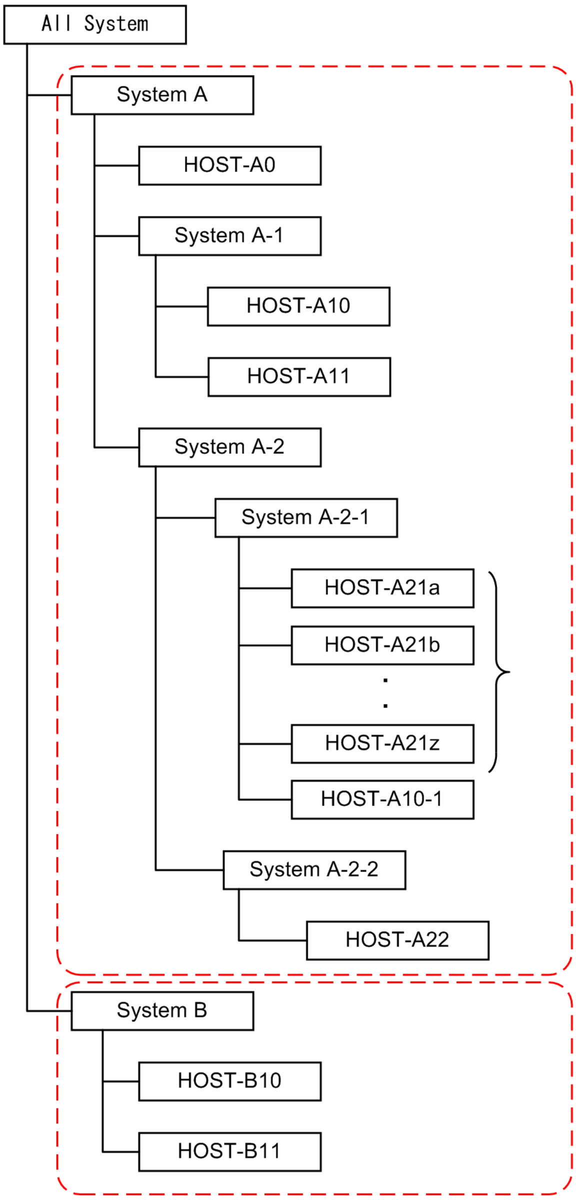
For details about hierarchical structures that can be represented in a sunburst or tree chart in the integrated operation viewer, see the section describing the hierarchical structure of a sunburst or tree chart in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Example definition 1

Definition of the example configuration

To define a structure that includes systems, subsystems, and their hosts described in the following figure:

Example configuration



Control access by using a JP1 resource group named `SYSTEM_A_User`.

Use a prefix to set a large number of hosts

Control access by using a JP1 resource group named `SYSTEM_B_User`.

```
{
  "meta":{
    "version":"2"
  },
  "allSystem":[
    {
      "id":"systemA",
      "displayName":"System A",
      "jp1ResourceGroup":"SYSTEM_A",
      "hostName":[{"HOST-A0":""}],
      "children":[
        {
          "id":"subA1",
          "displayName":"System A-1",
          "jp1ResourceGroup":"SYSTEM_A",
          "hostName":[{"HOST-A10":""},{"HOST-A11":""}]
        },
        {
          "id":"subA2",
          "displayName":"System A-2",
          "jp1ResourcesGroup":"SYSTEM_A",
          "children":[
            {
              "id":"subA21",
              "displayName":"System A-2-1",
              "jp1ResourcesGroup":"SYSTEM_A",
              "hostName":[{"^HOST-A21.*":"regexp"},{"HOST-A10-1":""}]
            },
            {
              "id":"subA22",
              "displayName":"System A-2-2",
              "jp1ResourcesGroup":"SYSTEM_A",
              "hostName":[{"HOST-A22":""}]
            }
          ]
        }
      ]
    },
    {
      "id":"systemB",
      "displayName":"System B",
      "jp1ResourcesGroup":"SYSTEM_B",
      "hostName":[{"HOST-B10":""},{"HOST-B11":""}]
    }
  ]
}
```

Example definition 2

Definition of a configuration where one host and root object node are used in more than one system or subsystem

As one host cannot be managed by more than one system, the host must be defined to be included in either System A or System B.

Example configuration

```
{
  "meta":{
    "version":"1"
  },
  "allSystem":[
    {
      "id":"systemA",
      "displayName":"System A",
      "hostName":[{"HOST1":""},{"HOST-A":""}]
    },
    {
      "id":"systemB",
      "displayName":"System B",
      "hostName":[{"HOST1":""},{"HOST-B":""}]
    }
  ]
}
```

Example definition to include the host in System A

```
{
  "meta":{
    "version":"1"
  },
  "allSystem":[
    {
      "id":"systemA",
      "displayName":"System A",
      "hostName":[{"HOST1":""},{"HOST-A":""}]
    },
    {
      "id":"systemB",
      "displayName":"System B",
      "hostName":[{"HOST-B":""}]
    }
  ]
}
```

Example definition to include the host in System B

```
{
  "meta":{
    "version":"1"
  },
  "allSystem":[
    {
      "id":"systemA",
      "displayName":"System A",
      "hostName":[{"HOST-A":""}]
    },
    {
      "id":"systemB",
      "displayName":"System B",
      "hostName":[{"HOST1":""},{"HOST-B":""}]
    }
  ]
}
```

Category name definition file for IM management nodes (imdd_category_name.conf)

Format

```
{
  "meta":{
    "version":"1"
  },
  "categoryData":[
    {"categoryId":"category-ID","categoryName":"category-name"},
    ...
  ]
}
```

Files

`imdd_category_name.conf`

`imdd_category_name.conf.model` (model file for the category name definition file for IM management nodes)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

This file defines the category names and orders of IM management nodes in management groups to display a sunburst or tree chart of data that is collected by the Intelligent Integrated Management Base. The IM management node categories are displayed in the order they are defined.

When the definitions are applied

The settings in the category name definition file for IM management nodes are applied to the Intelligent Integrated Management Base when the `jddcreatetree` or `jddupdatetree` command is completed successfully.

For details about the `jddcreatetree` and `jddupdatetree` commands, see *jddcreatetree* and *jddupdatetree* in *Chapter 1. Commands*.

Information that is specified

The category name definition file for IM management nodes must be saved in UTF-8 without BOM (byte order mark).

`"version":"1"`

Specifies the version of the category name definition file for IM management nodes. Set this to `1`.

`"categoryId":"`*category-ID*`"`

The specified default value. Do not edit the value.

`"categoryName":"`*category-name*`"`

Specifies a category name of the management group that will appear in a sunburst or tree chart. The value of `categoryName` can be up to 255 characters in length and must not include any control characters or machine-dependent characters.

Example definition

Example of the definition for changing the order of the underlined categories

Before the change

```
{
  "meta":{
    "version":"1"
  },
  "categoryData":[
    {"categoryId":"job","categoryName":"Job"},
    {"categoryId":"serviceResponse","categoryName":"Service Response"},
    {"categoryId":"enterprise","categoryName":"Enterprise"},
    {"categoryId":"transactionProcessing","categoryName":"Transaction Proces
sing"},
    {"categoryId":"applicationServer","categoryName":"Application Server"},
    {"categoryId":"database","categoryName":"Database"},
    {"categoryId":"platform","categoryName":"Platform"},
    {"categoryId":"virtualMachine","categoryName":"Virtual Machine"},
    {"categoryId":"managementApplications","categoryName":"Management Applic
ations"},
    {"categoryId":"otherApplications","categoryName":"Other Applications"}
  ]
}
```

After the change

```
{
  "meta":{
    "version":"1"
  },
  "categoryData":[
    {"categoryId":"job","categoryName":"Job"},
    {"categoryId":"serviceResponse","categoryName":"Service Response"},
    {"categoryId":"enterprise","categoryName":"Enterprise"},
    {"categoryId":"platform","categoryName":"Platform"},
    {"categoryId":"database","categoryName":"Database"},
    {"categoryId":"virtualMachine","categoryName":"Virtual Machine"},
    {"categoryId":"managementApplications","categoryName":"Management Applic
ations"},
    {"categoryId":"transactionProcessing","categoryName":"Transaction Proces
sing"},
    {"categoryId":"applicationServer","categoryName":"Application Server"},
    {"categoryId":"otherApplications","categoryName":"Other Applications"}
    ]
}
```

Target host definition file for configuration collection (imdd_target_host.conf)

Format

```
{
  "meta":{
    "version":"1"
  },
  "target":[
    {
      "product":"product-name",
      "hostName":["host-name-1","host-name-2",...]
    },
    ...
  ]
}
```

Files

`imdd_target_host.conf`

`imdd_target_host.conf.model` (model file for the target host definition file for configuration collection)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

When the Intelligent Integrated Management Base collects configuration data of the monitoring objects of the linked products, the hosts from which to collect data are set for each linked product based on this file.

When the definitions are applied

The settings in the target host definition file for configuration collection are applied to the Intelligent Integrated Management Base when the `jddcreatetree` and `jddupdatetree` commands are completed successfully.

For details about the `jddcreatetree` and `jddupdatetree` commands, see *jddcreatetree* and *jddupdatetree* in *Chapter 1. Commands*.

Information that is specified

The target host definition file for configuration collection must be saved in UTF-8 without BOM (byte order mark). If you specify a backslash (\) as part of a character string, immediately before \, specify \ as an escape character.

`"version":"1"`

Specifies the version of the target host definition file for configuration collection. Set this to `1`.

"product":"*product-name*"

Specifies an alphanumeric string to represent a product name to be linked. The maximum length is 255 characters. If a target host for configuration collection is specified, this option cannot be omitted.

- `AJS3`

  Specifies that JP1/AJS is linked.

- `PFM`

  Specifies that JP1/PFM is linked.

`"hostName":["`*host-name-1*`","`*host-name-2*`",...]`

Lists the names of hosts from which you want to collect configuration data with a string up to 255 characters.

Acceptable characters are alphanumeric characters and the following symbols: exclamation mark (!), dollar sign ($), left parenthesis ((), right parenthesis ()), asterisk (*), plus sign (+), comma (,), hyphen (-), period (.), forward slash (/), colon (:), left angle bracket (<), equal sign (=), left square bracket ([), backslash (\), right square bracket (]), caret (^), left curly bracket ({), vertical bar (|), and right curly bracket (}).

Specify physical host names or logical host names that are registered with the IM configuration. You cannot specify hosts with the same name within linked products. If a target host for configuration collection is specified, this option cannot be omitted.

Register the specified host name to the integrated manager's `hosts` file and DNS so as to enable name resolution on the integrated manager host. Configuration in the `jp1hosts` file and the `jp1hosts2` file are not referred.

Example definition

Example to link with JP1/AJS and JP1/PFM

```
{
  "meta":{
    "version":"1"
  },
  "target":[
    {
      "product":"AJS3",
      "hostName":["host-01","host-02","host-03"]
    },
    {
      "product":"PFM",
      "hostName":["host-01","host-04"]
    }
  ]
}
```

Host name definition file (imdd_host_name.conf)

Format

```
{
  "meta":{
    "version":"1"
  },
  "hostNameDef":[
    {
      "sourceHostName":["host-name-1-in-configuration-information","host-nam
e-2-in-configuration-information"],
      "hostName":"host-name-in-tree",
      "label":"display-name-on-screen"
    },
    ...
  ]
}
```

Files

`imdd_host_name.conf`

`imdd_host_name.conf.model` (model file for the host name definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

A structure of IM management nodes can include products that can have aliases for host names. In such a case, this file is used for mapping between aliases and real host names. If aliases are mapped to their real host name, the real host name is used as a host name in a tree chart. This allows the tree chart to group aliases into the same host even when different management tools use different aliases.

You also use this definition file when you change the host name displayed in the integrated operation viewer.

When the definitions are applied

The settings in the host name definition file are applied to the Intelligent Integrated Management Base when the `jddcreatetree` and `jddupdatetree` commands are completed successfully.

For details about the `jddcreatetree` and `jddupdatetree` commands, see *jddcreatetree* and *jddupdatetree* in *Chapter 1. Commands*.

Information that is specified

The host name definition file must be saved in UTF-8 without BOM (byte order mark). If you specify a backslash (\) as part of a character string, immediately before \, specify \ as an escape character.

`"version":"1"`

Specifies the version of the target host name definition file for configuration collection. Set this to `1`.

`"hostNameDef"`

Either `sourceHostName` or `label` must be specified. Specifying `hostName` is required.

`"sourceHostName":["`*host-name-1-in-configuration-information*`","`*host-name-2-in-configuration-information*`"]`

List the host names that you want to represent a particular host. You can specify up to 10 host names. Each host name can be up to 255 characters in length.

Acceptable characters are alphanumeric characters and the following symbols: exclamation mark (`!`), dollar sign (`$`), left parenthesis (`(`), right parenthesis (`)`), asterisk (`*`), plus sign (+), comma (`,`), hyphen (`-`), period (`.`), forward slash (`/`), colon (`:`), left angle bracket (<), equal sign (=), left square bracket (`[`), backslash (\), right square bracket (`]`), caret (`^`), left curly bracket (`{`), vertical bar (`|`), and right curly bracket (`}`).

`"hostName":"`*host-name-in-tree*`"`

Specify a host name in the tree data. The host name can be up to 255 characters in length.

Acceptable characters are alphanumeric characters and the following symbols: exclamation mark (`!`), dollar sign (`$`), left parenthesis (`(`), right parenthesis (`)`), asterisk (`*`), plus sign (+), comma (`,`), hyphen (`-`), period (`.`), forward slash (`/`), colon (`:`), left angle bracket (<), equal sign (=), left square bracket (`[`), backslash (\), right square bracket (`]`), caret (`^`), left curly bracket (`{`), vertical bar (`|`), and right curly bracket (`}`).

`"label":"`*display-name-on-screen*`"`

Specify a label name to be displayed on the screen. Specify it as a string no more than 255 characters, without any control and machine-dependent characters.

Host names displayed on the screen

Host names displayed on the screen are determined by the priorities as shown in the table below.

Priority	Matched with the value of `hostName`?	Is `label` specified?	Is `label` specified for the `value` value of the host configuration information SID?	Host name displayed on the screen
High	Match	Yes	--	The value of `label`
↑	Match	No	--	The value of `hostName`
↓	Unmatch	--	Yes	The value of `label` specified for the `value` value of the host configuration information SID
Low	Unmatch	--	No	The host name specified for the configuration information SID (*XXXXX* in `_HOST_`*XXXXX*)

Legend: --: Not applicable

You can see the configuration information SID and its `value` value in the Integrated Operation Viewer window or by using the REST API provided by JP1/IM - Manager. For details about SID, see *7.1 SID*, and for details about the REST API, see *5. API*.

Example definition

Example 1: Display `hostX` *as* `Host X` *on the screen*

```
{
  "meta":{
    "version":"1"
  },
  "hostNameDef":[
    {
      "hostName":"hostX",
      "label":"Host X"
    }
  ]
}
```

Example 2: Display `hostX` *as* `Host X` *on the screen when hosts defined as alias* `hostA` *and alias* `hostB` *are represented as* `hostX`

```
{
  "meta":{
    "version":"1"
  },
  "hostNameDef":[
    {
      "sourceHostName":["hostA","hostB"],
      "hostName":"hostX",
      "label":"Host X"
    }
  ]
}
```

IM management node link definition file (imdd_nodeLink_def.conf)

Format

```
{
  "meta":{
    "version":"1"
  },
  "links":[
    {
      "from":"configuration-information-SID-or-tree-SID-of-the-preceding-nod
e",
      "to":"configuration-information-SID-or-tree-SID-of-the-succeeding-node
",
      "type":"information-type"
      "value":{
        "unit":[
          {
              "precedingJob":"complete-name-of-preceding-linked-unit",
              "succeedingJob":"complete-name-of-subsequent-linked-unit",
              "succeedingJobTimeType":"format-of-scheduled-date-and-time-for
-linkage",
              "relationType":"type-of-linkage"
              ]
      }
    }, ...
  ]
}
```

Files

`imdd_nodeLink_def.conf`

`imdd_nodeLink_def.conf.model` (model file for the IM management node link definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

This file defines relationships between IM management nodes. You can use this definition file to define new relationships between IM management nodes. If you define the same relationship as that in the IM management node link file (imdd_nodeLink.json) (which is the one with the same from, to, and type), the relationship defined in this file takes effect in the system.

If JP1/AJS or JP1/PFM is linked, a relationship between monitoring targets is registered automatically by the related node display function. If you want to add other relationships separately and show them in the integrated operation viewer, you can specify them in this definition file. For details about the related node display function, see *3.11 Related node display function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you use the REST API, you can get the settings as data. For details about the REST API, see *5. API*.

When the definitions are applied

The settings in the IM management node link definition file are applied to the Intelligent Integrated Management Base when the jddupdatetree command is completed successfully.

Information that is specified

The IM management node link definition file must be saved in UTF-8 without BOM (byte order mark).

"version":"1"

Specifies the version of the IM management node link definition file. Set this to 1.

"from":"*configuration-information-SID-or-tree-SID-of-the-preceding-node*"

This node is the preceding node. Specify the configuration information SID or tree SID. For details about characters available for the type and name of SID, see *7.1 SID*. We recommend that you define the value you referred to in the Integrated Operation Viewer window or with the REST API.

This option is mandatory.

The **Job flow** tab displays relationships between IM management nodes only when rootJobnetExecutionOrder is specified for type and an SID is specified. If you specify a tree SID, you cannot view relationships between IM management nodes in the window. However, by using the link information acquisition API, you can acquire link information specified with the tree SID. For details, see *5.5.1 Link information acquisition*.

The **Related node** tab, on the other hand, displays relationships between IM management nodes regardless of the value specified for type or whether an SID or tree SID is specified.

Example to specify a root jobnet:

```
_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv/_JP1JOBG_jobgroup/_JP1R
OOTJOBNET_jobnet1
```

"to":"*configuration-information-SID-or-tree-SID-of-the-succeeding-node*"

This node is the subsequent node. Specify the configuration information SID or tree SID. For details about characters available for the type and name of SID, see *7.1 SID*. We recommend that you define the value you referred to in the Integrated Operation Viewer window or with the REST API.

This option is mandatory.

The **Job flow** tab displays relationships between IM management nodes only when rootJobnetExecutionOrder is specified for type and a SID is specified. If you specify a tree SID, you cannot view relationships between IM management nodes in the window. However, by using the link information acquisition API, you can acquire link information specified with the tree SID. For details, see *7.1 SID*.

The **Related node** tab, on the other hand, displays relationships between IM management nodes regardless of the value specified for type or whether an SID or tree SID is specified.

Example to specify a root jobnet:

```
_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv/_JP1JOBG_jobgroup/_JP1R
OOTJOBNET_jobnet2
```

`"type":"`*information-type*`"`

Specifies the type indicated by the link information set by `from` and `to`. Control characters are not acceptable. You can specify half-width alphanumeric characters from 1 to 255 bytes. This option is mandatory.

The `type` is the information used to group relationships with the same meaning. In the **Related node** tab of the Integrated Operation Viewer, you can view filtered relationships by `type`.

Use the types listed below within JP1/IM products or for linkage with other products. In addition to these types, you can also specify any type.

- `rootJobnetExecutionOrder` (relationship of execution order of a root jobnet)
- `managerAgent` (relationship between a manager and agent of a JP1 product)
- `rootJobnetAgent` (relationship between a root jobnet and an AJS agent)
- `sameNode` (relationship between nodes having the same name)
- `L2Connection` (relationship between layer-2 connection lines managed by JP1/NNMi)
- `Infrastructure` (relationship of infrastructure resources managed by JP1/OA)
- `monitoringConfiguration` (Relation between a product and a monitoring target in a monitoring product configuration)

If you set `type` to `rootJobnetExecutionOrder`, specify the configuration information SID of the IM management node for `from` and `to`.

`"value"`

Specifies additional link information. This option is optional.

`"unit"`

Specify it if the information type is an execution order of a root jobnet. Specify the information of a linked unit. This option is optional.

`"precedingJob":"`*complete-name-of-preceding-linked-unit*`"`

Specifies the complete name of a preceding linked unit. Specify a string of one megabyte or less other than control characters. This option is mandatory.

Example :

```
/jobnet1/JP1 event sending job
```

`"succeedingJob":"`*complete-name-of-subsequent-linked-unit*`"`

Specifies the complete name of a subsequent linked unit. Specify a string of one megabyte or less other than control characters. This option is mandatory.

Example :

```
/jobnet2/JP1 event reception monitoring job
```

`"succeedingJobTimeType":"`*format-of-scheduled-date-and-time-for-linkage*`"`

Specify it if the information type is an execution order of a root jobnet. Specify a scheduled date and time for linkage. This option is optional. If it is omitted, `endtime` is assumed for operation.

The specified option is ignored when `relationType` is set to `waitCondition`, and `startTime` is used for operation.

- `"startTime"`

Specify it if the link is configured so that execution of the subsequent unit is started after the preceding unit ends. For example, specify it for linkage through cancellation of holding operation.

- `"endTime"`

  Specify it if the link is configured so that the wait condition of the subsequent unit is met after the preceding unit ends. For example, use it for the link through event jobs (such as a file monitoring job or incoming email monitoring job).

`"relationType":"`*type-of-linkage*`"`

Specify it when the type of the target is the root jobnet execution order. Specify the type of linkage for `precedingJob` (full name of the preceding linked unit) and `succeedingJob` (full name of the subsequent linked unit).

- `waitCondition`

  Specify it for linkage with a wait.

  If you specify `waitCondition` for `relationType`, then specify the unit whose end is being waited for for `precedingJob` (complete name of the preceding linked unit), and specify the complete name of the unit with wait conditions for `succeedingJob` (complete name of the subsequent linked unit).

- `jobnetConnector`

  Specify it for linkage with a jobnet connector.

  If you specify `jobnetConnector` for `relationType`, then specify the job connector or the full name of the unit of the connection-destination root jobnet for `precedingJob` (complete name of the preceding linked unit) and `succeedingJob` (complete name of the subsequent linked unit).

- `other`

  Specify it for other linkages. For linkage with JP1 events, specify this value.

This option can be omitted. If you omit this option, `other` is assumed for operation.

Note that different dates and times appear in **Scheduled date and time for linkage** of the Linked unit dialog box depending on the specified types of linkage. For details, see the explanation on the linked unit in *2.6.1 Tabs area* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

Note

For `precedingJob` (complete name of the preceding linked unit) and `succeedingJob` (complete name of the subsequent linked unit), specify the full name of the unit corresponding to the type of linkage that is specified for `relationType` (type of linkage). If you specify the full name of the unit incorrectly, the correct date and time will not be displayed in **Scheduled date and time for linkage** in the Linked unit dialog box.

Example definition

```
{
    "meta":{
        "version":"1"
    },
        "links": [
    {
     "from":_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv
/_JP1JOBG_jobgroup/_JP1ROOTJOBNET_jobnet1",
     "to":_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv
/_JP1JOBG_jobgroup/_JP1ROOTJOBNET_jobnet2",
     "type":"rootJobnetExecutionOrder",
     "value":{
          "unit":[
           {
              "precedingJob":"/jobnet1/job1",
              "succeedingJob":"/jobnet2/Job2",
              "succeedingJobTimeType":"startTime"
              "relationType":"other"
           }, ...
         ]
      }

        }, ...
    ],
}
```

Suggestion definition file (imdd_suggestion.conf)

Format of the whole suggestion definition file

```
{
    "meta":{
        "version":"1"
    },
    "suggestions":[
        {
            "suggestionId":"suggestion-ID",
            "label":"label-name-of-the-suggestion",
            "node":"node-on-which-suggestion-information-is-shown",
            "permissions":[
                ["JP1-permission-for-showing-suggestion-information",...],
                ["JP1-permission-for-showing-suggestion-information",...],
                ...
            ],
            "cases":[
                [
                    "suggestion-activation-criteria",
                    "suggestion-activation-criteria",
                    ...
                ],
                [
                    "suggestion-activation-criteria",
                    "suggestion-activation-criteria",
                    ...
                ],
                ...
            ],
            "action":{
                "response-action-information"
            }
        },
        ...
    ]
}
```

Files

`imdd_suggestion_`*any-file-name*`.conf` (user-created suggestion definition file)

`imdd_suggestion.conf` (suggestion definition file)

`imdd_suggestion.conf.model` (model file for the suggestion definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\suggestion`

For a logical host:

shared-folder`\jp1imm\conf\imdd\suggestion`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/suggestion`

For a logical host:

shared-directory`/jp1imm/conf/imdd/suggestion`

For user-created suggestion definition files, copy the `imdd_suggestion.conf` file and store it in a given directory, and use the argument of the `jddupdatesuggestion` command to specify a directory path.

Description

A suggestion definition file defines criteria for suggesting response actions (suggestion display criteria and suggestion activation criteria) and what the actions do.

You can create more than one suggestion definition file. You can also create multiple suggestion definitions in one suggestion definition file. You should specify a suggestion ID (`suggestionId`) for each suggestion definition, so that it will be identified as an individual suggestion definition. Therefore, unique suggestion IDs must be specified in all suggestion definition files. If a specified suggestion ID is duplicated, an error occurs when the suggestion definition files are applied.

When the definitions are applied

When the `jddupdatesuggestion` command is completed successfully, the information in the suggestion definition file takes effect in the Intelligent Integrated Management Base.

Information that is specified

Save the suggestion definition file in UTF-8 format, with no byte order mark (BOM) added to it. The following shows the information that is specified in the whole suggestion definition file.

`"meta"`

Specifies meta information. The data type is object. This member cannot be omitted.

`"version":"1"`

Is the version of the suggestion definition file. Specify `1`. The data type is string. This member cannot be omitted.

`"suggestions"`

Is an array of suggestion definition objects. You can specify 0 to 1,000 definitions in a suggestion definition file (the total number of definitions for all suggestion definition files is 1,000). The data type is object[]. This member cannot be omitted.

`"suggestionId":"`*suggestion-ID*`"`

Specifies a unique suggestion ID throughout all suggestion definition files.

The suggestion ID can consist of half-width alphanumeric characters, hyphens (`-`), and underscores (_). You can specify from 1 to 255 characters.

Use an easy-to-understand suggestion ID because it is specified in a request for the REST API or used for message padding.

Note that in the suggestion list area on the **Suggestion** tab of the Integrated Operation Viewer window, the suggestions are sorted in order of activation status and character code of the suggestion ID. Therefore, define a suggestion ID with characters that come earlier in the character code order for a suggestion definition with higher priority.

Any string starting with `JP1`, `jp1`, `hitachi`, or `HITACHI` is not available for the suggestion ID.

The data type is string. This member cannot be omitted.

"label":"*label-name-of-the-suggestion*"

on the **Suggestion** tab of the Integrated Operation Viewer window and as **Suggestion name** in the **Suggestion details** area. You specify it as a string from 1 to 60 characters without any control characters. The data type is string. This member cannot be omitted.

"node":"*IM-management-node-on-which-suggestion-information-is-shown*"

Specifies the tree SID of the IM management node on which the suggestion is shown, with the regular expression. It can consist of half-width alphanumeric characters and symbols.

The suggestion information can be shown only on the IM management node with the tree SID that partially matches the specified regular expression. The data type is string. This member cannot be omitted.

"permissions":[["*JP1-user-permission-under-which-the-suggestion-information-is-shown*"]]

Specifies the JP1 user permission under which the suggestion information is shown in double arrays.

A set of conditions specified in interior square brackets ([]) is evaluated as an AND condition, whereas one specified in exterior square brackets is evaluated as an OR condition. You can specify 1 to 100 JP1 permissions as a combination of interior and exterior square brackets. The data type is string[][].

This member can be omitted. If it is omitted, the system follows the view condition for IM management nodes in the Integrated Operation Viewer window.

"cases":[["*suggestion-activation-criteria*"]]

Specifies information on suggestion activation criteria in double arrays.

A set of conditions specified in interior square brackets ([]) is evaluated as an AND condition, whereas one specified in exterior square brackets is evaluated as an OR condition. You can specify 1 to 100 sets of suggestion activation criteria as a combination of interior and exterior square brackets. The data type is object[][].

This member can be omitted. If it is omitted, the system assumes that the condition is always true.

"action":"*response-action-information*"

Specifies information on a response action. The data type is object. This member cannot be omitted.

You can use variables in the definition of suggestion activation criteria and response actions. For details about the use of variables, see *(3) Variables*.

(1) Suggestion activation criteria

Specify criteria when the suggestion function suggests response actions as suggestion activation criteria. Each criterion you specify has a *criterion key*, *comparison keyword*, and *value to be compared with*. Whether a criterion is true is determined by evaluating the target specified as the *criterion key* and the value specified as the *value to be compared with* using the comparison methods specified as the *comparison keyword*.

The suggestion activation criteria should be specified as an element of the cases parameter in the suggestion definition file. An interior array within the double array uses an AND condition, whereas an exterior array uses an OR condition. One AND-condition array is called a *suggestion activation criteria group*. The following shows an example of the suggestion activation criteria group:

```
cases:[
    [suggestion-activation-criterion-1,suggestion-activation-criterion-2]
,    <- Suggestion activation criteria group a
    [suggestion-activation-criterion-3,suggestion-activation-criterion-4
]     <- Suggestion activation criteria group b
]
```

In the above examples, suggestion activation criteria 1 and 2 are evaluated as an AND condition, whereas the suggestion activation criteria groups a and b are evaluated as an OR condition.

The suggestion activation criteria are evaluated in the order specified in the `cases` members. In the above example, the criteria are evaluated in the order of suggestion activation criterion 1, suggestion activation criterion 2, suggestion activation criterion 3, and suggestion activation criterion 4.

However, the evaluation can be skipped if a suggestion activation criteria group is not met or the suggestion activation criteria in the applicable suggestion definition are met.

For example, if a failed suggestion activation criterion is found in a suggestion activation criteria group, the evaluation is skipped even when some suggestion activation criteria have not been evaluated yet, because the suggestion activation criteria group is not met as an AND condition. If a suggestion activation criteria group is met, the evaluation is skipped even when some suggestion activation criteria groups have not been evaluated yet because the suggestion activation criteria in the applicable suggestion definition are met as an OR condition.

The following shows an example in which the evaluation of some suggestion activation criteria is skipped:

```
cases:[
    [suggestion-activation-criterion-1 (false), suggestion-activation-criter
ion-2 (skipped)],   <- Suggestion activation criteria group a
    [suggestion-activation-criterion-3 (true), suggestion-activation-criteri
on-4 (true)],     <- Suggestion activation criteria group b
    [suggestion-activation-criterion-5 (skipped), suggestion-activation-crit
erion-6 (skipped)]   <- Suggestion activation criteria group c
]
```

In the above example, when suggestion activation criterion 1 is determined to be false, suggestion activation criteria group a is not met and the evaluation of suggestion activation criterion 2 is skipped. When suggestion activation criteria 3 and 4 are determined to be true, suggestion activation criteria group b is met. This results in the suggestion activation criteria in the applicable suggestion definition being met, causing the evaluation of suggestion activation criteria 5 and 6 to be skipped.

Furthermore, if a suggestion activation criterion is determined to be an error due to a failure to get criterion information or to convert a variable, the suggestion activation criteria in the applicable suggestion definition are determined to be an error, causing all the subsequent evaluations to be skipped.

The following shows an example where all evaluations are skipped:

```
cases:[
    [<suggestion-activation-criterion-1(true)>, <suggestion-activation-crite
rion-2(error)>],
    [<suggestion-activation-criterion-3(skipped)>, <suggestion-activation-cr
iterion-4(skipped)>],
    [<suggestion-activation-criterion-5(skipped)>, <suggestion-activation-cr
iterion-6(skipped)>]
]
```

If suggestion activation criterion 2 is determined to be an error, then the suggestion activation criteria in the applicable suggestion definition are determined to be an error, causing the evaluations of suggestion activation criteria 3 to 6 to be skipped.

The `cases` members in interior `[]` are evaluated as an AND condition and those in exterior `[]` as an OR condition, and thus a set of OR conditions cannot be connected as an AND condition. To specify the same condition, you can rewrite the condition as follows:

(Before rewriting)

```
(condition A OR condition B) AND (condition C OR condition D)
```

(After rewriting)

```
(condition A AND condition C) OR (condition A AND condition D) OR (conditio
n B AND condition C) OR (condition B AND condition D)
```

Although you have to specify the same condition twice, it takes no time to evaluate it because the second evaluation uses the criterion information for evaluating the suggestion activation criterion obtained from JP1/IM or linked products at the time of the first evaluation.

If you want to connect AND and OR conditions in a complicated manner, you can also use plug-in functions or batch shell scripts to evaluate the conditions in these programs, in addition to the above method.

> **Note**
>
> If you want to check the criterion information acquired when judging the respective suggestion activation criteria (such as the standard output for a command or the REST API status code) when a suggestion is established, specify the variable of the suggestion activation criteria execution result in the `description` member of the response action. For details about variables, see *(3) Variable*.

Format of suggestion activation criterion

```
{
    "type":"type-of-criterion",
    "key":"criterion-key",
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified in a suggestion activation criterion

`"type":"`*type-of-criterion*`"`

Specifies the type of the suggestion activation criterion. For details about possible values, see the table below. The data type is string. This member cannot be omitted.

Table 2–6: Members available for type

No.	Value	Description
1	`event`	Specify it when you define a criterion for a JP1 event.
2	`eventCount`	Specify it when you define a criterion for the number of JP1 events.
3	`trendCount`	Specify it when you define a criterion for the number of time-series data sets.
4	`restApi`	Specify it when you define an execution result of the REST API.
5	`plugin`	Specify it when you define a criterion for an execution result of a product plug-in.
6	`cmd`#	Specify it when you define a criterion for an execution result of a command. For details about commands you can execute, the execution host, and the login user, see *4.5.10 jp1Imdd.execCmd*.
7	`struct`	Specify it when you define a criterion for IM management nodes.

#

You can specify this value when JP1/Base on the execution host for the command is version 12-10 or later. If the version is earlier than 12-10, the command execution fails, and the return value of 0 as well as empty standard output and standard error output are returned.

`"key":"`*criterion-key*`"`

Specifies the target of the suggestion activation criterion. Possible values vary depending on the value specified for the `type` member. The data type is object. This member cannot be omitted.

`"ope":"`*comparison-keyword*`"`

Specifies a keyword for comparison. Possible values vary depending on the value specified for the `type` member. The data type is string. This member cannot be omitted.

`"val":"`*value-to-be-compared-with*`"`

Specifies the value to be compared with. Possible values vary depending on the value specified for the `type` member. The data type depends on the `ope` member. This member cannot be omitted.

`"cache":"`*availability-of-criterion-information-cache*`"`

Specifies whether the cache of criterion information is used to evaluate the suggestion activation criterion.

- When the cache is used

  If a suggestion activation criterion is evaluated with the suggestion activation criterion having the same `key` before the cache expires, the information in the cache is used without getting the criterion information. The cache expires in 10 minutes.

- When the cache is not used

  Criterion information is always obtained to evaluate a suggestion activation criterion.

Specify either `true` or `false`. Specify `true` if you use the cache, or `false` if not.

This member is not available if the `type` member is set to `struct`. It is ignored if specified. When you specify `true`, the cache is created and updated when criterion information is obtained using the response action suggestion API.

The data type is Boolean. This member can be omitted. If it is omitted, the system assumes `false` for operation.

`"description":"`*description-of-the-criterion*`"`

Specifies the description of the suggestion activation criterion that is displayed in the **Suggestion details** area on the **Suggestion** tab of the Integrated Operation Viewer window, as a string from 1 to 512 characters without any control characters. The data type is string. This member cannot be omitted.

(A) Possible values for each of the key, ope, and val members

Different values can be specified for each of the `key`, `ope`, and `val` members depending on `type` (type of criterion) of a suggestion activation criterion. The possible values for each member are described here. Note that the `cache` and `description` members can be specified regardless of what `type` is.

(a) Suggestion activation criterion when type is set to event

When `type` (type of criterion) is set to `event`, whether any JP1 event that meets particular conditions exists can be specified as a suggestion activation criterion.

Format

```
{
    "type":"event",
    "key":{
        "sid":"tree-SID-of-the-node-with-which-the-event-is-associated",
        "statusFilter":status-of-node,
        "attribute-name":"attribute-value",
        "REGEX_attribute-name":"attribute-value"
    },
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on JP1 events which are subject to the suggestion activation criterion. The data type is object. This member cannot be omitted.

`"sid":"`*tree-SID-of-the-node-with-which-the-event-is-associated*`"`

Specifies the tree SID of the node with which the event is associated. Possible characters conform to the specifications of the tree SID. The data type is string. This member can be omitted. If it is omitted, the system assumes that the selected node is specified.

`"statusFilter":`*status-of-node*

Specifies the statuses of nodes as an array if you narrow down to only events that have applicable node statuses. Possible values are as follows:

- `10`: Green

  It narrows down events to processed events, released or deleted severe events, and events other than severe events.

- `20`: Yellow

  It narrows down events to severe events with the severity of `Warning`, `Debug`, and `Information` and the event status of `Unprocessed`, `Processing`, and `Held`.

- `30`: Orange

  It narrows down events to severe events with the severity of `Error` and the event status of `Unprocessed`, `Processing`, and `Held`.

- `40`: Red

  It narrows down events to severe events with the severity of `Emergency`, `Alert`, and `Critical` and the event status of `Unprocessed`, `Processing`, and `Held`.

When multiple values are specified, events are searched for in the OR condition.

When the severe events filter function or the severe event release and delete function is used to change events that correspond to the severe event, the events are narrowed down according to the status after the change when suggestion activation criteria are evaluated.

The data type is number[]. This member can be omitted. However, we recommend that you specify it in order to improve the performance of the event search.

`"`*attribute-name*`":"`*attribute-value*`"`

Specifies the value of the attribute specified by the attribute name for the event. The attribute names available as a member are the same as those values that can be specified for `key` in the event search condition object. The values that can be specified for each attribute name are the same as those values that can be specified for `val` in the search condition object. A single value can contain up to 4,096 bytes, and a single suggestion activation criterion can contain up to 4,096 bytes (total size of values specified for <*attribute-name*> and <`REG_`*attribute-name*> of a single suggestion activation criterion). For details about criterion information objects, see *7.2.1 (3)Event search condition object*. However, if a half-width space is specified in the value of each attribute, the system assumes that `%20` is specified.

An event that exactly matches the value is searched for. If the value is an array, an event that exactly matches one of the values is searched for.

If neither the attribute name `B.TIME` (registered time) nor the attribute name `B.ARRIVEDTIME` (arrived time) is specified, the system assumes that the following value is specified as a value of the attribute name `B.TIME`:

```
["one-day-before-the-current-time","current-time"]
```

If the attribute name `E.START_TIME` (start time) and the attribute name `E.END_TIME` (end time) have one of the following values, the system assumes no match, no matter what dates and times are specified:

- Value that is not a number
- Number less than 0
- Number of 4,102,444,800 or more

The data type depends on *attribute-name*. This member can be omitted.

`"REGEX_`*attribute-name*`":"`*attribute-value*`"`

Specifies the value of the attribute specified by *attribute-name* for the event. The attribute names available as a member are those values that can be specified for `key` of the event search condition object, which are attribute names for attributes containing a regular expression for the comparison keyword that can be specified. The values that can be specified for each attribute name are the same as those values that can be specified for `val` in the search condition object. A single value can contain up to 4,096 bytes, and a single suggestion activation criterion can contain up to 4,096 bytes (total size of values specified for <*attribute-name*> and <`REG_`*attribute-name*> of a single suggestion activation criterion). For details about criterion information objects, see *7.2.1 (3) Event search condition object*. However, if a half-width space is specified in the value of each attribute, the system assumes that `%20` is specified.

Events that partly match the value of the specified regular expression are searched for.

The data type is string. This member can be omitted.

`"ope":"`*comparison-keyword*`"`

Specifies a keyword for comparison. A possible value is as follows:

- `EXIST`: Whether JP1 events that meet all the conditions specified in `key` exist

The data type is string. This member cannot be omitted.

`"val":"`*value-to-be-compared-with*`"`

Specifies whether JP1 events that meet all the conditions specified in `key` exist.

Specify either `true` or `false`. Specify `true` if JP1 events exist, or `false` if they do not.

The data type is Boolean. This member cannot be omitted.

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

..

Example

Here is an example of evaluating whether JP1 events that meet the following conditions are issued:

- They are associated with the selected IM management node.
- Events that have the status of *Yellow* (`Warning`) or higher.
- The registration dates of the events are within the past 60 minutes.
- Their event ID is `00004860`, which is the one for the JP1/PFM health check event.

- The message of the event contains the health check status indicating that the host has stopped.
- The event status of the event is `Unprocessed`. (Its status is not `Processing` or `Held`.)

```
{
    "type":"event",
    "key":{
        "statusFilter":[20,30,40],
        "B.TIME":["${:time:-60.m.:}","${:time::}"],
        "B.ID":["00004860"],
        "REGEX_B.MESSAGE":"KAVL15022-E.*hcsstatus=Host Not Available",
        "E.@JP1IM_DEALT":[0]
    },
    "ope":"EXIST",
    "val":true,
    "description":"A JP1 event indicating that the host stopped has been i
ssued"
}
```

(b) Suggestion activation criterion when type is set to eventCount

When `type` (type of criterion) is set to `eventCount`, the number of JP1 events that meet particular conditions can be specified as a suggestion activation criterion.

Format

```
{
    "type":"eventCount",
    "key":{
        "sid":"tree-SID-of-the-node-with-which-the-event-is-associated",
        "statusFilter":status-of-node,
        "attribute-name":"attribute-value",
        "REGEX_attribute-name":"attribute-value"
    },
    "ope":"comparison-keyword",
    "val":value-to-be-compared-with,
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on JP1 events which are subject to the suggestion activation criterion. The data type is object. This member cannot be omitted.

`"sid":"`*tree-SID-of-the-node-with-which-the-event-is-associated*`"`

This is an object that specifies the information on JP1 events which are subject to the suggestion activation criterion. The data type is string. This member can be omitted. If it is omitted, the system assumes that the selected node is specified.

`"statusFilter":`*status-of-node*

Specifies the statuses of nodes as an array if you narrow down to only events that have applicable node statuses. Possible values are as follows:

- `10`: Green

It narrows down events to processed events, released or deleted severe events, and events other than severe events.

- `20`: Yellow

  It narrows down events to severe events with the severity of `Warning`, `Debug`, and `Information` and the event status of `Unprocessed`, `Processing`, and `Held`.

- `30`: Orange

  It narrows down events to severe events with the severity of `Error` and the event status of `Unprocessed`, `Processing`, and `Held`.

- `40`: Red

  It narrows down events to severe events with the severity of `Emergency`, `Alert`, and `Critical` and the event status of `Unprocessed`, `Processing`, and `Held`.

When multiple values are specified, events are searched for in the OR condition.

When the severe events filter function or the severe event release and delete function is used to change events that correspond to the severe event, the events are narrowed down according to the status after the change when suggestion activation criteria are evaluated.

The data type is number[]. This member can be omitted. However, we recommend that you specify it in order to improve the performance of the event search.

`"attribute-name":"`*attribute-value*`"`

Specifies the value of the attribute specified by the attribute name for the event. The attribute names available as a member are the same as those values that can be specified for `key` in the event search condition object. The values that can be specified for each attribute name are the same as those values that can be specified for `val` in the search condition object. A single value can contain up to 4,096 bytes, and a single suggestion activation criterion can contain up to 4,096 bytes (total size of values specified for <*attribute-name*> and <`REG_`*attribute-name*> of a single suggestion activation criterion). For details about criterion information objects, see *7.2.1 (3) Event search condition object*. However, if a half-width space is specified in the value of each attribute, the system assumes that `%20` is specified.

An event that exactly matches the value is searched for. If the value is an array, an event that exactly matches one of the values is searched for.

If neither the attribute name `B.TIME` (registered time) nor the attribute name `B.ARRIVEDTIME` (arrived time) is specified, the system assumes that the following value is specified as a value of the attribute name `B.TIME`:

```
["one-day-before-the-current-time","current-time"]
```

If the attribute name `E.START_TIME` (start time) and the attribute name `E.END_TIME` (end time) have one of the following values, the system assumes no match, no matter what dates and times are specified:

- Value that is not a number
- Number less than 0
- Number of 4,102,444,800 or more

The data type depends on *attribute-name*. This member can be omitted.

`"REGEX_`*attribute-name*`":"`*attribute-value*`"`

Specifies the value of the attribute specified by *attribute-name* for the event. The attribute names available as a member are those values that can be specified for `key` of the event search condition object, which are attribute names for attributes containing a regular expression for the comparison keyword that can be specified. The values that can be specified for each attribute name are the same as those values that can be specified for `val` in the search condition object. A single value can contain up to 4,096 bytes, and a single suggestion activation criterion can contain up to 4,096 bytes (total size of values specified for <*attribute-name*> and <`REG_`*attribute-name*> of a single suggestion activation criterion). For details about criterion information objects, see *7.2.1 (3) Event search condition object*. However, if a half-width space is specified in the value of each attribute, the system assumes that `%20` is specified.

Events that partly match the value of the specified regular expression are searched for.

The data type is string. This member can be omitted.

`"ope":"`*comparison-keyword*`"`

Specifies a keyword for comparison. Possible values are as follows:

- `GT`: The number of JP1 events that meet the conditions specified in `key` is greater than the value specified in `val`.
- `LT`: The number of JP1 events that meet the conditions specified in `key` is less than the value specified in `val`.

The data type is string. This member cannot be omitted.

`"val":`*value-to-be-compared-with*

Specifies the number of JP1 events that meet the conditions specified in `key`, as an integer from 0 to 100.

The data type is number. This member cannot be omitted.

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether more than 10 JP1 events that meet the following conditions are issued:

- They are associated with the selected IM management node.
- Events that have the status of *Yellow* (`Warning`) or higher.
- The registration dates of the events are within the past 60 minutes.
- Their event ID is `00004860`, which is the one for the JP1/PFM health check event.
- The message of the event contains the health check status indicating that the host has stopped.
- The event status of the event is `Unprocessed`. (Its status is not `Processing` or `Held`.)

```
{
    "type":"eventCount",
    "key":{
        "B.TIME":["${:time:-60.m.:}","${:time::}"],
        "B.ID":["00004860"],
        "REGEX_B.MESSAGE":"KAVL15022-E.*hcsstatus=Host Not Available",
        "E.@JP1IM_DEALT":[0]
    },
    "ope":"GT",
    "val":10,
    "description":"More than 10 JP1 events indicating that the host has st
opped have been issued within the past one hour"
}
```

(c) Suggestion activation criterion when type is set to trendCount

When `type` (type of criterion) is set to `trendCount`, the number of time-series data sets that meet particular conditions can be specified as a suggestion activation criterion.

Format

```
{
    "type":"trendCount",
    "key":{
        "sid":"tree-SID",
        "metric":"metric-name",
        "startTime":"start-date-and-time",
        "endTime":"end-date-and-time",
        "countPerInstance":upper-limit-for-the-number-of-data-sets-per-ins
tance,
        "instanceCount":upper-limit-for-the-number-of-instances,
        "instance":"instance-name",
        "threshold":threshold-value,
        "thresholdType":"threshold-value-type"
    },
    "ope":"comparison-keyword",
    "val":value-to-be-compared-with,
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

"key"

This is an object that specifies the information on time-series data which is subject to the suggestion activation criterion.

The data type is object. This member cannot be omitted.

"sid":"*tree-SID*"

Specifies the tree SID of time-series data. Possible characters conform to the specifications of the tree SID.

If multiple configuration information SIDs are associated with the specified tree SID, the time-series data from one configuration information SID is obtained.

If the time-series data is obtained successfully, it is used to evaluate the conditions. If obtaining it fails, the next time-series data is obtained.

When time-series data is unable to be obtained for all configuration information SIDs, obtaining criterion information is a failure. The order of obtaining time-series data is undefined.

The data type is string. This member can be omitted. If it is omitted, the system assumes that the selected node is specified.

"metric":"*metric-for-time-series-data*"

Specifies a metric for time-series data. You specify it with half-width alphanumeric characters, hyphens (-), and underscores (_) of 255 characters or fewer. The data type is string. This member cannot be omitted.

"startTime":"*start-date-and-time-of-the-time-series-data*"

Specifies the start date and time of time series data as the UTC time in ISO 8601 format. Do not specify the seconds after the decimal point. The data type is string. This member cannot be omitted.

"endTime":"*end-date-and-time-of-the-time-series-data*"

Specifies the end date and time of time-series data as the UTC time in ISO 8601 format. Do not specify the seconds after the decimal point. The data type is string. This member cannot be omitted.

"countPerInstance":*upper-limit-for-the-number-of-data-sets-per-instance*

Specifies the upper limit for the number of data sets per instance to be obtained. An integer from 1 to 30,000 can be specified. Specify it so that the number obtained by multiplying countPerInstance by instanceCount is 30,000 or less. The data type is number. This member can be omitted. If it is omitted, the system assumes 60 for operation.

`"instanceCount"`:*upper-limit-for-the-number-of-instances*

Specifies the upper limit for the number of instances. An integer from 1 to 30,000 can be specified. Specify it so that the number obtained by multiplying `countPerInstance` by `instanceCount` is 30,000 or less. The data type is number. This member can be omitted. If it is omitted, the system assumes 10 for operation.

`"instance"`:`"`*instance-name*`"`

Specifies the instance name of the instance that is subject to the suggestion activation criterion when there are multiple instances in the time-series data. The data type is string. This member can be omitted. If it is omitted, the first instance is subject to the suggestion activation criterion.

A string of up to 255 characters without any control character can be specified.

`"threshold"`:*threshold-value*

Specifies the threshold value for the target time-series data. The data type is number. This member cannot be omitted.

`"thresholdType"`:`"`*threshold-value-type*`"`

Specifies the range of the target time-series data. Possible values are as follows:

- <: The range of targets is less than the value specified for `threshold`.
- <=: The range of targets is less than or equal to the value specified for `threshold`.
- >: The range of targets is more than the value specified for `threshold`.
- >=: The range of targets is more than or equal to the value specified for `threshold`.

The data type is string. This member cannot be omitted.

`"ope"`:`"`*comparison-keyword*`"`

Specifies a keyword for comparison. Possible values are as follows:

- `GT`: The number of time-series data sets that meet the conditions specified in `key` is greater than the value specified in `val`.
- `LT`: The number of time-series data sets that meet the conditions specified in `key` is less than the value specified in `val`.

The data type is string. This member cannot be omitted.

`"val"`:*value-to-be-compared-with*

Specifies the number of time-series data sets that meet the conditions specified in `key`. An integer from 0 to 30,000 can be specified. The data type is number. This member cannot be omitted.

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether one or more time-series data sets that meet the following conditions exist:

- Target node: Selected node
- Metric: CPU usage
- Start date and time: One hour ago
- End date and time: Current time
- Upper limit for the number of data sets per instance: 60
- Upper limit for the number of instances: 10
- Threshold value: 80

- Threshold value type: Greater than the threshold value

```
{
    "type":"trendCount",
    "key":{
        "sid":"${.:tree:sid:}",
        "metric":"cpu_used_rate",
        "startTime":"${:time:-60.m.:}",
        "endTime":"${:time::}",
        "countPerInstance":60,
        "instanceCount":10,
        "threshold":80,
        "thresholdType":">"
    },
    "ope":"GT",
    "val":0,
    "description":"One or more time-series data sets that exceeded 80% ar
e found in the time-series data of CPU usage for the past one hour"
}
```

(d) Suggestion activation criterion when type is set to restApi

When `type` (type of criterion) is set to `restApi`, the execution result of the REST API (the status code, response header, and response body) can be specified as a suggestion activation criterion.

Format

```
{
    "type":"restApi",
    "key":{
        "method":"method-of-the-REST-API",
        "url":"URL-of-the-REST-API",
        "headers":"request-header-of-the-REST-API",
        "body":"request-body-of-the-REST-API",
        "param":"parameter-to-be-compared-with-in-the-response-of-the-REST
-API"
    },
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on the REST API which is subject to the suggestion activation criterion.

The data type is object. This member cannot be omitted.

`"method":"`*method-of-the-REST-API*`"`

Specifies a method of the REST API. Possible values are as follows:

- `GET`
- `HEAD`
- `POST`

- PUT
- PATCH
- DELETE
- OPTIONS
- TRACE

The data type is string. This member cannot be omitted.

"url":"*URL-of-the-REST-API*"

Specifies the URL of the REST API. Possible characters are half-width alphanumeric characters and the following symbols that conform to the RFC 2396 specifications:

;, /, ?, :, @, &, =, +, $, ,, -, _, ., !, ~, *, ', (,), %

Begin the URL with http:// or https://.

The data type is string. This member cannot be omitted.

When the URL including host name is specified, register the host name to the integrated manager's hosts file and DNS so as to enable name resolution on the integrated manager host. Configuration in the jp1hosts file and the jp1hosts2 file are not referred.

"headers":"*request-header-of-the-REST-API*"

Specifies the request header of the REST API. The data type is object. This member cannot be omitted.

"body":"*request-body-of-the-REST-API*"

Specifies the request body of the REST API. The data type is object. When the GET or DELETE method is used and the body is not required, omit this member. This member can be omitted.

"param":"*parameter-to-be-compared-with-in-the-response-of-the-REST-API*"

Specifies the parameter to be compared with in the response of the REST API. Possible values are as follows:

- status: Status code
- headers: Response header
- body: Response body

The data type is string. This member cannot be omitted.

"ope":"*comparison-keyword*"

Specifies a keyword for comparison. Possible values are as follows:

- IN: The response of the REST API specified in key matches the value specified for val.
- NOTIN: The response of the REST API specified in key does not match the value specified for val.
- GT: The response of the REST API specified in key is greater than the value specified for val.
- LT: The response of the REST API specified in key is less than the value specified for val.
- REGEX: The response of the REST API specified in key partly matches the value specified for val by a regular expression.

The data type is string. This member cannot be omitted.

"val":"*value-to-be-compared-with*"

Specifies the value to be compared with the execution result of the REST API. Possible values vary depending on the value of param. For details, see the table below. If the type is string, specify a string of less than 1 megabyte in size. This member cannot be omitted.

Table 2–7: Combinations of param, ope, and the type of val available for restApi

No.	param value	Value available for ope	Type of val	Value to be specified for val
1	`status`	• `IN` • `NOTIN` • `GT` • `LT`	number	Value to be compared with the status code of the REST API
2	`headers`	• `IN` • `NOTIN` • `REGEX`	string	Value to be compared with the response header of the REST API
3	`body`	• `IN` • `NOTIN` • `REGEX`	string	Value to be compared with the response body of the REST API

Format of the string for the REST API response header

When `param` is set to `headers`, the response header obtained will be a string in the following format:

```
<field-name-1>:<field-value-1-1>,<field-value-1-2>,...,<field-value-1-n><C
RLF>
<field-name-2>:<field-value-2-1>,<field-value-2-2>,...,<field-value-2-n><C
RLF>
<field-name-3>:<field-value-3-1>,<field-value-3-2>,...,<field-value-3-n><C
RLF>
...
```

Note: All the field names are converted into uppercase characters. The fields are arranged in ascending order of the field names in ASCII code.

The following shows an example of how they are specified:

```
CACHE-CONTROL:no-store,no-cache,max-age=0<CRLF>
CONTENT-TYPE:application/json<CRLF>
EXPIRES:Thu,01 Jan 1970 00:00:00 GMT<CRLF>
PRAGMA:no-cache<CRLF>
```

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether the status code of the following REST API is 200:

- Method: `POST`
- URL: `https://test`
- Request header
  Authentication information: `yyyy/zzzz`
  Media type of the request body: `application/json`
- Request body
  Request body parameter `body1`: `test1`
  Request body parameter `body2`: `test2`
- Parameter to be compared with in the REST API response: Status code

```
{
    "type":"restApi",
    "key":{
        "method":"POST",
        "url":"https://test",
        "headers":{
            "Authorization":"yyyy/zzzz",
            "Content-Type":"application/json"
        },
        "body":{
            "body1":"test1",
            "body2":"test2"
        },
        "param":"status"
    },
    "ope":"IN",
    "val":200,
    "description":"The status code of REST API test is 200"
}
```

(e) Suggestion activation criterion when type is set to plugin

When `type` (type of criterion) is set to `plugin`, the execution result of the plug-in function can be specified as a suggestion activation criterion.

Format

```
{
    "type":"plugin",
    "key":{
        "sid":"tree-SID",
        "method":"name-of-the-plug-in-function",
        "args":"arguments-of-the-plug-in-function"
    },
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on the plug-in function which is subject to the suggestion activation criterion. The data type is object. This member cannot be omitted.

`"sid":"`*tree-SID*`"`

Specifies the tree SID. Possible characters conform to the specifications of the tree SID. The plug-in function is executed by specifying the configuration information SID associated with the specified tree SID. If multiple configuration information SIDs are associated with the specified tree SID, the plug-in function is executed by specifying one configuration information SID, and if it is executed successfully, the criterion is evaluated with the response of the plug-in function. The subsequent configuration information SIDs are ignored.

The order of specifying configuration information SIDs is undefined.

If the `args.setError` method is executed in the plug-in, or if `suggestion` is not found in the member of the response, a failure in the execution of the plug-in function is determined, resulting in execution of the plug-in function with the next configuration information SID.

If the execution of the plug-in function fails with the all configuration information SIDs, obtaining criterion information fails. The data type is string. This member can be omitted. If it is omitted, the system assumes that the selected node is specified.

`"method":"`*name-of-the-plug-in-function*`"`

Specifies the name of the plug-in function. After adding the plug-in function, check if the JP1/IM3-Manager service is restarted. The plug-in function to be specified must meet all of the following conditions:

- It is modularized in `module.exports`.
- It has only the `args` argument of object type.
- It returns the response with the `args.setResult(Object result)` method, not with `return`. Specify the response for `result`.
- It notifies an error with the `args.setError(String message)` method, not via an exception. Specify the error message for `message`.
- `suggestion` (data type: string) is found in the member of the response.

The data type is string. This member cannot be omitted.

For details about the plug-in function, see *4. User-created Plug-ins*.

`"args":"`*arguments-of-the-plug-in-function*`"`

Specifies arguments of the plug-in function to be executed. If there is no information to pass, specify an empty object. The specified object is passed to the `args.methodArgs` argument of the plug-in function to be executed. For details about other values passed to `args` of the plug-in function, see *5.7.1 Plug-in processing execution*.

The data type is object. This member cannot be omitted.

`"ope":"`*comparison-keyword*`"`

Specifies a keyword for comparison. Possible values are as follows:

- `IN`: The value of `suggestion` in the response of the plug-in function specified in `key` matches the value specified for `val`.
- `NOTIN`: The value of `suggestion` in the response of the plug-in function specified in `key` does not match the value specified for `val`.
- `REGEX`: The value of `suggestion` in the response of the plug-in function specified in `key` partly matches the value specified for `val` by a regular expression.

The data type is string. This member cannot be omitted.

`"val":"`*value-to-be-compared-with*`"`

Specifies the value to be compared with the value of `suggestion` in the response of the plug-in function. Specify a string of less than 1 megabyte in size. The data type is string. This member cannot be omitted.

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether the `suggestion` member of the following plug-in function has the OK value:

- Target IM management node: Selected IM management node

- Plug-in function: `jp1pfmSuggestionCreateReportURL`
  The function creates the URL of a JP1/PFM report. For details about the `jp1pfmSuggestionCreateReportURL` function, see the *JP1/Performance Management Reference*.
- Argument: ID of the report

```
{
    "type":"plugin",
    "key":{
        "sid":"${.:tree:sid:}",
        "method":"jp1pfmSuggestionCreateReportURL",
        "args":{
            "reportId":"ac102ce0:3b9952:ec20ca1bfc:-7b99"
         }
    },
    "ope":"NOTIN",
    "val":"",
    "description":"Successful creation of the report URL"
}
```

(f) Suggestion activation criterion when type is set to cmd

When `type` (type of criterion) is set to `cmd`, the execution result of the command (the return value, standard output, and standard error output) can be specified as a suggestion activation criterion.

Format

```
{
    "type":"cmd",
    "key":{
        "host":"execution-host-name-of-the-command",
        "cmd":"command-to-be-executed",
        "env":"environment-variables",
        "envFile":"environment-variable-file-name",
        "param":"type-of-the-command-execution-result"
    },
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "cache":"availability-of-criterion-information-cache",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on the command which is subject to the suggestion activation criterion. The data type is object. This member cannot be omitted.

`host:"`*execution-host-name-of-the-command*`"`

Specifies the execution host name of the command. The range allowed is from 1 to 254 bytes. The data type is string. This member cannot be omitted.

`"cmd":"`*command-to-be-executed*`"`

Specifies the command to be executed and its arguments. The range allowed is from 1 to 4,095 bytes.

Enclose the command name containing any space characters in double quotation marks (`"`). The data type is string. This member cannot be omitted.

"env":"*environment-variables*"

Specifies the environment variable values as the value of the object, using the environment variables when the command is executed on the execution host as the key of the object.

You can specify up to 30 variables. Specify the keys and values of the objects in the range from 1 to 7,107 bytes in total. The data type is object. This member can be omitted.

"envFile":"*environment-variable-file-name*"

Specifies the name of the file on the execution host in absolute path format. The range allowed is from 1 to 255 bytes. The data type is string. This member can be omitted.

"param":"*value-to-be-compared-with*"

Specifies the target to be compared with. Possible values are as follows:

- rc: Return value
- stdout: Standard output
- stderr: Standard error output

The data type is string. This member cannot be omitted.

"ope":"*comparison-keyword*"

Specifies a keyword for comparison. Possible values are as follows:

- IN: The value of param for the command specified in key matches the value specified for val.
- NOTIN: The value of param for the command specified in key does not match the value specified for val.
- REGEX: The value of param for the command specified in key partly matches the value specified for val by a regular expression.
- GT: The value of param for the command specified in key is greater than the value specified for val.
- LT: The value of param for the command specified in key is less than the value specified for val.

For details about the combinations of param and ope available, see *Table 2-8*.

The data type is string. This member cannot be omitted.

"val":"*value-to-be-compared-with*"

Specifies the value to be compared with the execution result of the command. Possible values vary depending on the value specified for param. For details, see the table below. Note that if the type is string, you must specify a string of less than 1 megabyte in size. This member cannot be omitted.

Table 2–8: Combinations of param, ope, and the type of val available for cmd

No.	param value	Value available for ope	Type of val	Value to be specified for val
1	rc	• IN • NOTIN • GT • LT	number	Value to be compared with the return value of the command
2	stdout	• IN • NOTIN • REGEX	string	Value to be compared with the standard output from the command
3	stderr	• IN • NOTIN • REGEX	string	Value to be compared with the standard error output from the command

If a variable is specified in a suggestion activation criterion with the `type` of `cmd`, the following character conversion is performed after the conversion of the variable:

- If the variable specified in the suggestion activation criterion contains any of the following control characters, it is converted into a half-width space character (0x20):
  - 0x01 to 0x1F (except a tab (0x09))
  - 0x7F
- The character conversion is performed according to the configuration file for converting information. For details, see *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files*.

For details about the `cache` and `description` members, see the description for each member in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether the standard output from the command with the following conditions contains `DISPLAY_NAME: JP1/AJS service` (whether the JP1/AJS service is running).

- Execution host name of the command: Node name of the selected IM management node#
  #: Node of the JP1/AJS manager host
- Command to be executed: `sc query`
- Environment variable file name: `C:\envFile.txt` on the target host
- Type of the command execution result: Standard output

```
{
    "type":"cmd",
    "key":{
        "host":"${.:tree:value.label:}",
        "cmd":"sc query",
        "envFile":"C:\\envFile.txt",
        "param":"stdout"
    },
    "ope":"REGEX",
    "val":"DISPLAY_NAME: JP1/AJS3",
    "description":"The JP1/AJS service is running"
}
```

(g) Suggestion activation criterion when type is set to struct

When `type` (type of criterion) is set to `struct`, whether the configuration of a specific IM management node exists can be specified as a suggestion activation criterion.

Format

```
{
    "type":"struct",
    "key":{
        "idType":"type-of-the-node",
        "sid":"configuration-information-SID-or-tree-SID"
    },
    "ope":"comparison-keyword",
    "val":"value-to-be-compared-with",
    "description":"description-of-the-criterion"
}
```

Information that is specified

`"key"`

This is an object that specifies the information on the IM management node which is subject to the suggestion activation criterion. The data type is object. This member cannot be omitted.

`"idType":"`*type-of-the-node*`"`

Specifies the ID type of the target node. Possible values are as follows:

- `target`: Configuration information SID
- `tree`: Tree SID

The data type is string. This member cannot be omitted.

`"sid":"`*configuration-information-SID-or-tree-SID*`"`

Specifies the configuration information SID or tree SID. Possible characters conform to the SID specifications.

If the conversion of the variable specified as an `sid` member fails, the system considers the SID as not existing, instead of regarding the evaluation as a failure, and continues processing when the conversion failure is caused by either of the following:

- The target node does not exist.
- The target type is set to `target` or `target[`*product-name*`]`, but the SID of the applicable configuration information does not exist.

The data type is string. This member cannot be omitted.

`"ope":"`*comparison-keyword*`"`

Specifies a keyword for comparison. A possible value is as follows:

- `EXIST`: Whether the IM management node that meets the conditions specified in `key` exists

The data type is string. This member cannot be omitted.

`"val":"`*value-to-be-compared-with*`"`

Specifies whether the IM management node with the conditions specified in `key` exists.

Specify either `true` or `false`. Specify `true` if the IM management node exists, or `false` if it does not.

The data type is Boolean. This member cannot be omitted.

For details about the `description` member, see the description in *(1) Suggestion activation criteria*.

Example

Here is an example of evaluating whether the IM management node of JP1/AJS - Agent on the same host as the selected IM management node of JP1/PFM - Agent exists.

- ID type: Tree SID
- SID: SID that meets the following conditions:
- A tree SID agrees with that of the selected JP1/PFM - Agent in the part of the tree SID from the beginning to the three-level higher IM management node (IM management node of the host).
- The tree SID after the host is the following tree SID that indicates JP1/AJS-Agent: `_CATEGORY_managementApplications/_OBJECT_JP1AJSAGT`

```
{
    "type":"struct",
    "key":{
        "idType":"tree",
        "sid":"${../../..:tree:sid:}/_CATEGORY_managementApplications/_OBJ
ECT_JP1AJSAGT"
    },
    "ope":"EXIST",
    "val":true,
    "description":"A node of JP1/AJS - Agent exists on the same host as th
e selected IM management node of JP1/PFM - Agent"
}
```

(2) Response action

The following describes the response action.

Response action format

```
{
    "type":"type-of-response-action",
    "params":"parameters-of-the-response-action",
    "description":"description-of-the-response-action"
}
```

Response action definition

`"type":"`*type-of-response-action*`"`

Specifies the type of response action. Possible values are as follows:

- `restApi`: Specify this type when you define the execution of the REST API.
- `plugin`: Specify this type when you define the execution of a product plug-in.
- `cmd`: Specify this type when you define the execution of a command.
- `eventStatus`: Specify this type when you define the change in the event status of an event.
- `jump`: Specify this type when you define a jump to a particular URL or the Repeated event list window.

The data type is string. This member cannot be omitted.

Note that you specify `cmd` when JP1/Base on the execution host of the command is version 12-10 or later. If the version is earlier than 12-10, the command execution fails, and the return value of 0 as well as empty standard output and standard error output are returned.

`"params":"`*parameters-of-the-response-action*`"`

Specifies the parameters of the response action. Possible members vary depending on `type`. The data type is object. This member cannot be omitted.

`"description":"`*description-of-the-response-action*`"`

Specifies the description of the response action. A string of up to 512 characters without any control character can be specified. An empty string is not allowed.

The data type is string. This member cannot be omitted.

(A) Possible values for each response action type

Different values can be specified for members depending on `type` (response action type) of the response action. The following describes the values available for each `type`. Note that you can specify the `description` member regardless of what `type` is.

(a) Response action when type is set to restApi

When `type` (response action type) is set to `restApi`, the execution of the REST API can be specified as response action.

Format

```
{
    "type":"restApi",
    "params":{
        "method":"method-of-the-REST-API",
        "url":"URL-of-the-REST-API",
        "headers":"request-header-of-the-REST-API",
        "body":"request-body-of-the-REST-API"
    },
    "description":"description-of-the-response-action"
}
```

Information that is specified

`"params"`

This is an object that specifies the information on the REST API on which the response action is taken. The data type is object. This member cannot be omitted.

`"method":"`*method-of-the-REST-API*`"`

Specifies a method of the REST API. Possible values are as follows:

- `GET`
- `HEAD`
- `POST`
- `PUT`
- `PATCH`
- `DELETE`
- `OPTIONS`
- `TRACE`

The data type is string. This member cannot be omitted.

`"url":"`*URL-of-the-REST-API*`"`

Specifies the URL of the REST API. Possible characters are half-width alphanumeric characters and the following symbols that conform to the RFC 2396 specifications:

`;`, `/`, `?`, `:`, `@`, &, =, +, `$`, `,`, `-`, _, `.`, `!`, ~, `*`, `'`, `(`, `)`, `%`

Begin the URL with `http://` or `https://`.

The data type is string. This member cannot be omitted.

When the URL including host name is specified, register the host name to the integrated manager's `hosts` file and DNS so as to enable name resolution on the integrated manager host. Configuration in the `jp1hosts` file and the `jp1hosts2` file are not referred.

`"headers":"`*request-header-of-the-REST-API*`"`

Specifies the request header of the REST API. The data type is object. This member cannot be omitted.

"body":"*request-body-of-the-REST-API*"

Specifies the request body of the REST API. When the GET or DELETE method is used and the body is not required, omit this member. The data type is object. This member can be omitted.

For details about the description member, see the description in *(2) Response action*.

Example

Here is an example of executing the REST API with the following JP1 event information:

- URL: https://test
- Request header

  Authentication information: yyyy/zzzz

  Media type of the request body: application/json
- Request body

  Request body parameter body1: ${:event[1]:B.ID:}

  This is the event ID of the JP1 event that meets the first suggestion activation criterion with type specified for cases set to event.
- Request body parameter body2: ${:event[1]:B.MESSAGE:}

  This is the message of the JP1 event that meets the first suggestion activation criterion with type specified for cases set to event.

```
{
    "type":"restApi",
    "params":{
        "method":"POST",
        "url":"https://test",
        "headers":{
            "Authorization":"yyyy/zzzz",
            "Content-Type":"application/json"
        },
        "body":{
            "body1":"${:event[1]:B.ID:}",
            "body2":"${:event[1]:B.MESSAGE:}"
        }
    },
    "description":"Use JP1 event information to execute a REST API test"
}
```

(b) Response action when type is set to plugin

When type (response action type) is set to plugin, the execution of a plug-in function can be specified as response action.

Format

```
{
    "type":"plugin",
    "params":{
        "sid":"tree-SID",
        "method":"name-of-the-plug-in-function",
        "args":"arguments-of-the-plug-in-function"
    },
    "description":"description-of-the-response-action"
}
```

Information that is specified

`"params"`

This is an object that specifies the information on the plug-in function on which the response action is taken. The data type is object. This member cannot be omitted.

`"sid":"`*tree-SID*`"`

SID. The plug-in function is executed by specifying the configuration information SID associated with the specified tree SID. If multiple configuration information SIDs are associated with the specified tree SID, the plug-in function is executed by specifying one configuration information SID, and if it is executed successfully, the subsequent configuration information SIDs are ignored. The order of specifying configuration information SIDs is undefined.

If the `args.setError` method is executed in the plug-in, a failure in the execution of the plug-in function is determined, resulting in execution of the plug-in function with the next configuration information SID.

The data type is string. This member can be omitted. If it is omitted, the system assumes that the selected node is specified.

`"method":"`*name-of-the-plug-in-function*`"`

Specifies the name of the plug-in function. After adding the plug-in function, check if the JP1/IM3-Manager service is restarted. The plug-in function to be specified must meet all of the following conditions:

- It is modularized in `module.exports`.
- It only has the `args` argument of object type.
- It returns the response with the `args.setResult(Object result)` method, not with `return`.

  Specify the response for `result`.
- It notifies an error with the `args.setError(String message)` method, not via an exception.

  Specify the error message for `message`.
- The function name does not start with two underscores (__).

The data type is string. This member cannot be omitted.

`"args":"`*arguments-of-the-plug-in-function*`"`

Specifies arguments of the plug-in function to be executed. If there is no information to pass, specify an empty object. The specified object is passed to the `args.methodArgs` argument of the plug-in function to be executed. For details about other values passed to `args` of the plug-in function, see *5.7.1 Plug-in processing execution*.

The data type is object. This member cannot be omitted.

For details about the `description` member, see the description in *(2) Response action*.

Example

Here is an example of executing the plug-in function under the following conditions:

- Target IM management node: Selected IM management node
- Plug-in function: `jp1pfmSuggestionSetStatusOfEventsToProcessed`

  This function turns a JP1 event into processed. For details about the `jp1pfmSuggestionSetStatusOfEventsToProcessed` function, see the *JP1/Performance Management Reference*.

- Argument: Event SID

  This is the value of response `suggestion` of the plug-in function that was executed under the third suggestion activation criterion with `type` specified for `cases` set to `plugin`.

```
{
    "type":"plugin",
    "params":{
        "sid":"${.:tree:sid:}",
        "method":"jp1pfmSuggestionSetStatusOfEventsToProcessed",
        "args":{
            "eventSids":"${:plugin[3]::}"
        }
    },
    "description":"Turn the alarm or the event status of the event on an a
gent in normal status into Processed"
}
```

If linkage with JP1/PFM is enabled, the plug-in methods of JP1/PFM will be available. For details, see the *JP1/Performance Management User's Guide*.

(c) Response action when type is set to cmd

When `type` (response action type) is set to `cmd`, the execution of the command can be specified as response action.

Format

```
{
    "type":"cmd",
    "params":{
        "host":"execution-host-of-the-command",
        "cmd":"command-to-be-executed",
        "env":"environment-variables",
        "envFile":"environment-variable-file-name"
    },
    "description":"description-of-the-response-action"
}
```

Information that is specified

`"params"`

This is an object that specifies the information on the command on which the response action is taken. The data type is object. This member cannot be omitted.

`"host":"`*execution-host-of-the-command*`"`

Specifies the execution host name of the command. The range allowed is from 1 to 254 bytes. The data type is string. This member cannot be omitted.

`"cmd":"`*command-to-be-executed*`"`

Specifies the command to be executed and its arguments. The range allowed is from 1 to 4,095 bytes.

Enclose the command name containing any space characters in double quotation marks ("). The data type is string. This member cannot be omitted.

`"env":"`*environment-variables*`"`

Specifies the environment variable values as the value of the object, using the environment variables when the command is executed on the execution host as the key of the object.

You can specify up to 30 variables. Specify the keys and values of the objects in the range from 1 to 7,107 bytes in total. The data type is object. This member can be omitted.

`"envFile":"`*environment-variable-file-name*`"`

Specifies the name of the file on the execution host in absolute path format. The range allowed is 1 to 255 bytes. The data type is string. This member can be omitted.

If a variable is specified in a response action with the `type` of `cmd`, the following character conversion is performed after the conversion of the variable:

- If the variable specified in a response action contains any of the following control characters, it is converted into a half-width space character (0x20):
  - 0x01 to 0x1F (except a tab (0x09))
  - 0x7F
- The character conversion is performed according to the configuration file for converting information. For details, see *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files*.

For details about the `description` member, see the description in *(2) Response action*.

Example

Here is an example of executing the command under the following conditions:

- Execution host name of the command: Node name of the selected IM management node (node of a JP1/IM host)
- Command to be executed: `"C:\Program Files (x86)\Hitachi\JP1IMM\tools\jim_log" -f C:\\temp -q`

  This is the data collection command of JP1/IM.
- Environment variable file name: `C:\envFile.txt` on the target host

```
{
    "type":"cmd",
    "params":{
        "host":"${.:tree:value.label:}",
        "cmd":"\"C:\\Program Files (x86)\\Hitachi\\JP1IMM\\tools\\jim_log\
" -f C:\\temp -q",
        "envFile":"C:\\envFile.txt"
    },
    "description":"Execution of the data collection command of JP1/IM"
}
```

(d) Response action when type is set to eventStatus

When `type` (response action type) is set to `eventStatus`, a change in the event status of a JP1 event can be specified as response action.

Format

```
{
    "type":"eventStatus",
    "params":{
        "dealt":event-status,
        "sid":"JP1-event-SID,..."
    },
    "description":"description-of-the-response-action"
}
```

Information that is specified

"params"

This is an object that specifies the event and its event status on which the response action is taken. The data type is object. This member cannot be omitted.

"dealt":*event-status*

Specifies the new event status. The following values can be specified:

- 0: Unprocessed
- 1: Processed
- 2: Processing
- 3: Held

The data type is number. This member cannot be omitted.

"sid":"*JP1-event-SID*"

Specifies the SIDs of JP1 events whose status you want to get.

If you specify SIDs of multiple JP1 events, use commas (,) to concatenate the SIDs of the JP1 events. Possible characters conform to the SID specifications. You can specify SIDs of events from 1 to 2,000. The data type is string. This member cannot be omitted.

For details about the description member, see the description in *(2) Response action*.

Example

Here is an example of changing the event status of an event to 1 (Processed) under the following condition:

- Event SID: ${:event[1]:sid:},${:event[2]:sid:}

  This is the event SID of the JP1 event that meets the first and second suggestion activation criteria with type specified for cases set to event.

```
{
    "type":"eventStatus",
    "params":{
        "dealt":1,
        "sid":"${:event[1]:sid:},${:event[2]:sid:}"
    },
    "description":"Change the event ID: ${:event[1]:B.ID:}, ${:event[2]:B.
ID:} to Processed"
}
```

(e) Response action when type is set to jump

When type (response action type) is set to jump, a jump to a particular URL or the Repeated event list window can be specified as a response action.

Format

```
{
    "type":"jump",
    "params":{
        "url":"URL",
        "target":"target-attribute-of-HTML",
        "relatedEvent":repeated-event-list-window-information
    },
    "description":"description-of-the-response-action"
}
```

Information that is specified

`"params"`

This is an object that specifies the information on the jump destination on which the response action is taken. The data type is object. This member cannot be omitted.

`"url":"`*URL*`"`

Specify the URL of a jump destination in either of the following formats.

Possible characters are half-width alphanumeric characters and the following symbols that conform to the RFC 2396 specifications:

`;`, `/`, `?`, `:`, `@`, `&`, `=`, `+`, `$`, `,`, `-`, `_`, `.`, `!`, `~`, `*`, `'`, `(`, `)`, `%`

Begin the URL with one of `http://`, `https://`, or `index?`.

- Any URL

  Specify a given URL.

- Direct access URL of JP1/IM

  Specify a direct access URL of JP1/IM by using `index` in the Integrated Operation Viewer window. The window currently open jumps to the specified URL, without refreshing the window. For details about the format of the direct access URL, see *4.12 Setting up the direct access URL* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

The data type is string. You must specify either this member or the `relatedEvent` member.

`"target":"`*target-attribute-of-HTML*`"`

Specify the HTML `target` attribute when the URL of the jump destination is opened. If it is omitted, the system assumes that `_blank` is specified. The following values cannot be specified:

- `_self`
- `_parent`
- `_top`
- Value starting with `JP1IM_`

If the `url` member is omitted or a URL starting with `index` is specified for the value of the `url` member, the value of the `target` member is ignored. The data type is string. This member can be omitted.

`"relatedEvent":`*search-criterion-number*

Specify it when you show the Repeated event list window. The target events are those that are searched for under the suggestion activation criteria with `type` set to `event`. Specify a suggestion activation criterion number from 1 to 100 of suggestion activation criteria with `type` specified for `cases` set to `event`.

If more than one JP1 event that meets the criterion is found, the Repeated event list window for the JP1 event with the latest registration date and time is displayed.

The data type is number. You must specify either this member or the `url` member.

For details about the `description` member, see the description in *(2) Response action*.

Example 1

Here is an example of jumping to a specific URL by specifying a target name:

```
{
    "type":"jump",
    "params":{
        "url":"https://sample/web/application",
        "target":"sampleWebApplication"
    },
    "description":"Jump to https://sample/web/application"
}
```

Example 2

Here is an example of specifying a direct access URL:

```
{
    "type":"jump",
    "params":{
        "url":"index?sid=${../../..:tree:sid:URLENC}%2F%5FCATEGORY%5Fmanag
ementApplications%2F%5FOBJECT%5FJP1AJSAGT&view=tree&eou=1"
    },
    "description":"Screen transition of JP1/IM (JP1/AJS - Manager node on
the same host)"
}
```

Example 3

Here is an example of specifying the Repeated event list window:

```
{
    "type":"jump",
    "params":{
        "relatedEvent":1
    },
    "description":"Open the Repeated event list window"
}
```

(3) Variable

You can specify variables for suggestion activation criteria and response actions. With variables, the information and current time of the selected IM management node can be replaced with the information obtained when the suggestion activation criterion is evaluated. The use of variables allows you to dynamically define suggestion activation criteria and response actions.

Example of specifying suggestion activation criteria with variables

Suggestion activation criteria

- Suggestion activation criterion 1: A JP1 event with the event ID of xxx exists.
- Suggestion activation criterion 2: JP1 events with the registration date and time that falls on or after *the registration date and time of the event which meets suggestion activation criterion 1* exists.

Define *the registration date and time of the event which meets suggestion activation criterion 1* as a variable. When a variable is specified in suggestion activation criteria, it is converted when each suggestion activation criterion is evaluated. If the evaluation is skipped, the variable is not converted. For details about skipping the evaluation, see the description in *(1) Suggestion activation criteria*.

Variables specified in a response action are converted after suggestion criteria of the response action are evaluated. If the evaluation result is false, the variables are not converted.

Example

```
"cases":[
  ["suggestion-activation-criterion-1","suggestion-activation-criterion
-2"],
  ["suggestion-activation-criterion-3"]
],
"action":"response-action"
```

In the above example, the processing is performed in the following order:

1. Convert variables specified in suggestion activation criterion 1
2. Evaluate suggestion activation criterion 1 (true)
3. Convert variables specified in suggestion activation criterion 2
4. Evaluate suggestion activation criterion 2 (false)
5. Convert variables specified in suggestion activation criterion 3
6. Evaluate suggestion activation criterion 3 (true)
7. Convert variables specified in the response action
8. Suggest the response action

You can specify variables in suggestion activation criteria, string-type members of response actions (other than `type`), string-type elements of arrays, and string-type members of objects (except for the member name). The format of a variable is as follows:

```
${"target-node":"type-of-target":"target-key":"encoding-type"}
```

Important

The colons (`:`) in the variable format cannot be omitted. Furthermore, `$`, `{`, and `}` are not available in the target node. `:`, `$`, `{`, and `}` are not available in the type of target, the target key, and the encoding type.

(A) Target node

Specify the IM management node from which information is obtained, in the relative path format from the tree SID or the selected IM management node. It can be omitted depending on the type of conversion target of the variable. For details, see *Table 2-10 Possible values for the type of target*. If a target node is specified for the type of target that does not require it, it is ignored.

The table below describes the format of the relative path. Use slashes (`/`) for concatenation.

Table 2–9: Format of the relative path

No.	Format of the relative path	Node indicated when specified at the beginning of the target node	Node indicated when specified after the first slash (/) of the target node
1	`.`	Specify it to indicate the selected IM management node or the node of the tree SID specified by the request of the response action suggestion API.	Not available.
2	`..`	Specify it to indicate the upper-level node of the selected IM management node or the upper-level node of the tree SID specified by the request of the response action suggestion API.	Specify it to indicate the upper-level node of the current node.
3	Structured identifier	Specify a structured identifier in the absolute path to specify a node in the absolute path format.	Specify the structured identifiers of subsequent tree SIDs of the current node to specify a lower-level node of the current node.

No.	Format of the relative path	Node indicated when specified at the beginning of the target node	Node indicated when specified after the first slash (/) of the target node
		For details about possible characters in the structured identifier, see *7.1 SID*.	For details about possible characters in the structured identifier, see *7.1 SID*.
4	*link-direction<linkType>*	Not available.	Specify it to indicate a related node by using the current node and the link for the type of link information <*linkType*>. You can specify whichever link information of the tree SID or the configuration information SID. You can specify either of the following for *link-direction*: • <: Preceding node • >: Succeeding node `Tree` cannot be specified for <*linkType*>. In addition, if there are multiple links that correspond to *link-direction<linkType>*, the system assumes that the related node of the first link is specified for operation. For details about characters available in <*linkType*>, see the description of `type` (*information-type*) in *IM management node link definition file (imdd_nodeLink_def.conf)* in *Chapter 2. Definition Files*.

(B) Type of target

In the type of target, specify the type of target of conversion, i.e., how a variable is converted, such as when a variable is converted into event information or a REST API execution result. The following table describes the values available for the type of target.

Table 2–10: Possible values for the type of target

No.	Type of target	Description	Necessity of specifying the target node
1	`target[`*product-name*`]`	A variable is converted into the SID information of configuration information created by the product plug-in of `[`*product-name*`]` in the SIDs of the configuration information of the target node. If the target node has multiple SIDs of configuration information created by the product plug-in of the target, a variable is converted into the SID information of the configuration information obtained first. The order of obtaining the information is undefined. You can omit `[`*product-name*`]`. If it is omitted, a variable is converted into the SID information of the configuration information obtained first. The order of obtaining the information is also undefined in this case. The value specified `[`*product-name*`]` can accept the same value that can be specified for `product` in the target host definition file for configuration collection. For details, see *Target host definition file for configuration collection (imdd_target_host.conf)* in *Chapter 2. Definition Files*.	Required
2	`tree`	A variable is converted into the information of the tree SID of the target node.	Required
3	`time`	A variable is converted into the time information.	Optional
4	`event[`*n*`]`	A variable is converted into the information of the JP1 event that meets the *n*th suggestion activation criterion in the suggestion activation criteria with `type` specified for `cases` set to `event`.	Optional

No.	Type of target	Description	Necessity of specifying the target node
		If multiple JP1 events meet the criterion, a variable is converted into the information of the JP1 event with the most recent registration date and time. Specify a number from 1 to 100 for `[n]`.	
5	`eventCount[n]`	A variable is converted into the information of the JP1 event that meets the *n*th suggestion activation criterion in the suggestion activation criteria with `type` specified for `cases` set to `eventCount`. If multiple JP1 events meet the criterion, a variable is converted into the information that contains the information of all applicable JP1 events altogether. Specify a number from 1 to 100 for `[n]`.	Optional
6	`restApi[n]`	A variable is converted into the information of the response of the REST API executed under the *n*th suggestion activation criterion in the suggestion activation criteria with `type` specified for `cases` set to `restApi`. Specify a number from 1 to 100 for `[n]`.	Optional
7	`plugin[n]`	A variable is converted into the information of the execution result of the plug-in function executed under the *n*th suggestion activation criterion in the suggestion activation criteria with `type` specified for `cases` set to `plugin`. Specify a number from 1 to 100 for `[n]`.	Optional
8	`cmd[n]`	A variable is converted into the information of the execution result of the command executed under the *n*th suggestion activation criterion in the suggestion activation criteria with `type` specified for `cases` set to `cmd`. Specify a number from 1 to 100 for `[n]`.	Optional

(C) Target key

For the target key, specify an element for the type of target of which a variable is converted. For example, specify the status code element or body element of the response for the execution of the REST API. The value that can be specified for the target key varies depending on the type of target. The following explains the target key you can specify for each type of target.

(a) When the type of target is target

When the type of target is `target`, specify the SID element of configuration information for the target key. Possible target keys are as follows:

`sid`

A variable is converted into the value of the configuration information SID of the target node.

`value.`*member-name*

A variable is converted into the value of the member specified as *member-name* for the `value` value assigned to the configuration information SID of the target node.

If you want to specify more members in the object, specify them in the following format:

```
object-name.member-name
```

However, they cannot be specified if the specified member is of an array or object type.

If you convert the value of a property configured by the product plug-in that appears in the **Properties** for the related node area on the **Related node** tab in the Integrated Operation Viewer window, specify it in the following format:

```
value.property.property-name
```

Example

Here is an example of obtaining the service ID from the SID of the selected IM management node (IM management node of the JP1/PFM agent) and executing the command to suspend monitoring.

Note that it assumes that the service ID has been obtained by specifying the following values in variables:

- Target node: Selected IM management node
- Type of target: `target` (Configuration information SID)
- Target key: `value.property.SerViceId` (`ServiceId` member of `property` in the `Value` value)

```
{
    "type":"cmd",
    "params":{
        ...
        "cmd":"\"C:\\Program Files (x86)\\Hitachi\\jp1pc\\tools\\jpctool\
" monitor suspend -noquery -id ${.:target:value.property.ServiceId:}"
    },
    "description":"Execute the command to suspend monitoring of JP1/PFM"
}
```

(b) When the type of target is tree

When the type of target is `tree`, specify the SID element of the tree for the target key. Possible target keys are as follows:

`sid`

A variable is converted into the SID value of the tree of the target node.

`value.`*member-name*

A variable is converted into the value of the member specified as *member-name* for the `value` value assigned to the tree SID of the target node.

If you want to specify more members in the object, specify them in the following format:

```
object-name.member-name
```

However, members of an array or object type cannot be specified.

Example

Here is an example of specifying the tree SID of the selected node:

```
{
    "type":"event",
    "key":{
        "sid":"${.:tree:sid:}",
        ...
    },
    ...
}
```

(c) When the type of target is time

When the type of target is `time`, specify the relative date and time from the current time (UTC time in ISO 8601 format) for the target key. The relative date and time is specified in the following format:

```
[+|-]value.unit.segmentation
```

You can omit the target key. If it is omitted, a variable is converted into the current date and time in ISO 8601 format. Possible target keys for `time` are as follows:

`[+|-]`

Specify whether the target key is in the future or in the past based on the current date and time.

- `+`: The target key is converted into a future date and time.
- `-`: The target key is converted into a past date and time.

You can omit this key. If it is omitted, a variable is converted into the current time.

value`.`*unit*

Specify how far the time is in the future or past from the current date and time.

Specify an integer from 1 to 2147483647 as the value. Specify one of the following values as the unit:

- `y`: Year
- `M`: Month
- `d`: Day
- `h`: Hour
- `m`: Minute
- `s`: Second

When `[+|-]` is omitted, this key cannot be specified. When `[+|-]` is specified, this key cannot be omitted. Note that an error occurs if the variable is converted into the following date and time:

- Date and time before 1970-01-01T00:00:00Z
- Date and time after 9999-12-31T23:59:59Z

segmentation

Specify a segmented part of a specified date and time if you want to convert only part of the date and time. The following values can be specified:

- `y`: Year part
- `M`: Month part
- `d`: Day part
- `h`: Hour part
- `m`: Minute part
- `s`: Second part

You can omit this key. If it is omitted, the whole date and time is converted.

Example

Here is an example of specifying events in the time period from yesterday's 23:00 UTC to today's 2:00 UTC under an event criterion.

Note that it assumes that the following combination of variables has been used to get *yesterday's 23:00 UTC* and *today's 2:00 UTC*.

Yesterday's 23:00 UTC

- `${:time:-1.d.y:}` Year part of the date one day before the current time
- `${:time:-1.d.M:}` Month part of the date one day before the current time
- `${:time:-1.d.d:}` Day part of the date one day before the current time

These variables get the value of *segmentation* of the date one day before the current time by specifying `time` for the type of target and `-1.d.`*segmentation* for the target key.

Today's 2:00 UTC

- `${:time:..y:}` Year part of the current time
- `${:time:..M:}` Month part of the current time
- `${:time:..d:}` Day part of the current time

These variables get the value of *segmentation* of the current date and time by specifying `time` for the type of target and *segmentation* for the target key.

```
{
    "type":"event",
    "key":{
        "B.TIME":["${:time:-1.d.y:}-${:time:-1.d.M:}-${:time:-1.d.d:}T23:0
0:00Z", "${:time:..y:}-${:time:..M:}-${:time:..d:}T02:00:00Z"],
            ...
    },
    ...
}
```

(d) When the type of target is event[n]

When the type of target is `event[`*n*`]`, specify the JP1 event element for the target key. Possible target keys are as follows:

`sid`

A variable is converted into the SID of the JP1 event.

attribute-name

A variable is converted into the attribute value of <*attribute-name*> of the JP1 event. For details about possible attribute names, see *5.6.1 Event search*.

Example

Here is an example of specifying the conditions where the event ID of the unprocessed event of `YYYY` has been issued after the event ID of the unprocessed event of `XXXX` under event criteria.

Note that it assumes that the condition of the `YYYY` event after `XXXX` has been specified by designating the registration date and time of the event that meets the first event criterion for the first element of `B.TIME` (registration time) of the second event criterion and designating the current time as the second element. Also note that it assumes that the registration date and time of the event that meets the first event criterion is obtained by specifying the following values for the variables:

- Type of target: `event[1]` First event criterion
- Target key: `B.TIME` Registration date and time of the event

```
"cases":[
    [
        {
            "type":"event",
            "key":{
                "sid":"${.:tree:sid:}",
                "statusFilter":[30],
                "B.ID":["XXXX"],
                "E.@JP1IM_DEALT":[0]
            },
            ...
        },
        {
            "type":"event",
            "key":{
                "sid":"${.:tree:sid:}",
                "statusFilter":[30],
                "B.TIME":["${:event[1]:B.TIME:}","${:time::}"],
                "B.ID":["YYYY"],
                "E.@JP1IM_DEALT":[0]
            },
            ...
        }
    ]
]
```

(e) When the type of target is eventCount[n]

When the type of target is `eventCount[`*n*`]`, specify the JP1 event element for the target key. Possible target keys are as follows:

`sid`

A variable is converted into the SID of the JP1 event. If multiple JP1 events meet the criterion, it is converted into a string with each event separated by a comma (`,`).

Example

Here is an example of using the response action for changing the event statuses of JP1 events to change all JP1 events that meet the event criterion to `Processed`.

```
{
    "type":"eventStatus",
    "params":{
        "sid":"${:eventCount[1]:sid:}",
        "dealt":1
    },
    "description":"Change all the applicable JP1 events to Processed"
}
```

(f) When the type of target is restApi[n]

When the type of target is `restApi[`*n*`]`, specify the response of the REST API for the target key. Possible target keys are as follows:

`status`

A variable is converted into the status code of the response of the REST API.

`headers`

A variable is converted into the response header of the REST API. For details about the format after the conversion, see the description in *Format of the string for the REST API response header* of *(1)(d) Suggestion activation criterion when type is set to restApi*.

`body`

A variable is converted into the response body of the REST API.

Example

Here is an example of specifying the response body of the REST API executed under a REST API criterion, as an argument of the response action on the execution of a plug-in function.

Note that it assumes that the response body of the REST API executed under the REST API criterion is obtained by specifying the following values for the variables:

- Type of target: `restApi[1]` First REST API criterion
- Target key: `body` Response body

```
"cases":[
    [
        {
            "type":"restApi",
            ...
        }
]
...

"action": {
    "type":"plugin",
    "params":{
        ...
        "args":{
            "apiResponse":"${:restApi[1]:body:}"
        }
    },
    ...
}
```

(g) When the type of target is plugin[n]

When the type of target is `plugin[n]`, you do not have to specify the target key. The plug-in function specified in `key` of a suggestion activation criterion is converted into the value of the `suggestion` member in the object passed to the `args.setResult` method.

Example

Here is an example of specifying the response of the plug-in function executed under a plug-in criterion, as an argument of the response action on the execution of a plug-in function.

Note that it assumes that the response of the plug-in function executed under the plug-in criterion is obtained by specifying the following values for the variables:

- Type of target: `plugin[1]` Plug-in function criterion
- Target key: Not specified

```
"cases":[
    [
        {
            "type":"plugin",
            ...
        }
]
...

"action": {
    "type":"plugin",
    "params":{
        ...,
        "args":{
            "pluginResult":"${:plugin[1]::}"
        }
    },
    ...
}
```

(h) When the type of target is cmd[n]

When the type of target is `cmd[n]`, specify the execution result element of the command for the target key. Possible target keys are as follows:

`rc`

A variable is converted into the return value of the command.

`stdout`

A variable is converted into the standard output of the command.

`stderr`

A variable is converted into the standard error output of the command.

Example

Here is an example of specifying the standard output of the command executed under a command execution criterion, as an argument of the response action on the execution of a plug-in function.

Note that it assumes that the standard output of the command executed under the command execution criterion is obtained by specifying the following values for the variables:

- Type of target: `cmd[1]` First command criterion
- Target key: `stdout` Standard output

```
"cases":[
    [
        {
            "type":"cmd",
            ...
        }
]
...

"action": {
    "type":"plugin",
    "params":{
        ...,
        "args":{
            "cmdStdOut":"${:cmd[1]:stdout:}"
        }
    },
    ...
}
```

(i) Encoding type

Specify the encoding type when you encode variables when they are converted. You can omit the encoding type. If it is omitted, the variables are not encoded.

Possible encoding types are as follows:

- `ENC`: The variables are Base64-encoded.

- URLENC: The variables are URL-encoded.

Notes

- Grant the Administrator permissions in Windows, or the root permissions in UNIX, to the suggestion definition file.
- You can use regular expressions in the suggestion definition file. In this case, it may take time for mapping if you make heavy use of .*, which matches all characters. When you use .*, place the regular expression only where needed.
- Regular expressions in the suggestion definition file use partial matching, and thus an expression with .* at the beginning and end indicates the same condition as one without .* at the beginning and end.

  For example, examples 1 and 2 below are the same condition:

  Example 1: Regular expression that matches a string that contains _OBJECT_JP1IMMGR

  .*_OBJECT_JP1IMMGR.*

  Example 2: Regular expression that matches a string that contains _OBJECT_JP1IMMGR

  _OBJECT_JP1IMMGR

  It may take time for search if .* is placed at the beginning and end, so avoid specifying .* there.
- If either of the following conditions is met when regular expressions are used, the KAJY22042-W message is displayed when the jddupdatesuggestion command is executed:
  - As a regular expression, .* is placed at the beginning or at the end.
  - As a regular expression, consecutive use of .* is made.

  For details about the KAJY22042-W message, see the *JP1/Integrated Management 3 - Manager Messages*.
- It may take time to evaluate suggestion activation criteria depending on the amount of suggestion information that is displayed on one IM management node. Perform trial operation adequately until you are sure that there is no problem.

Definition example

The following explains a definition example of the suggestion definition file under the conditions below.

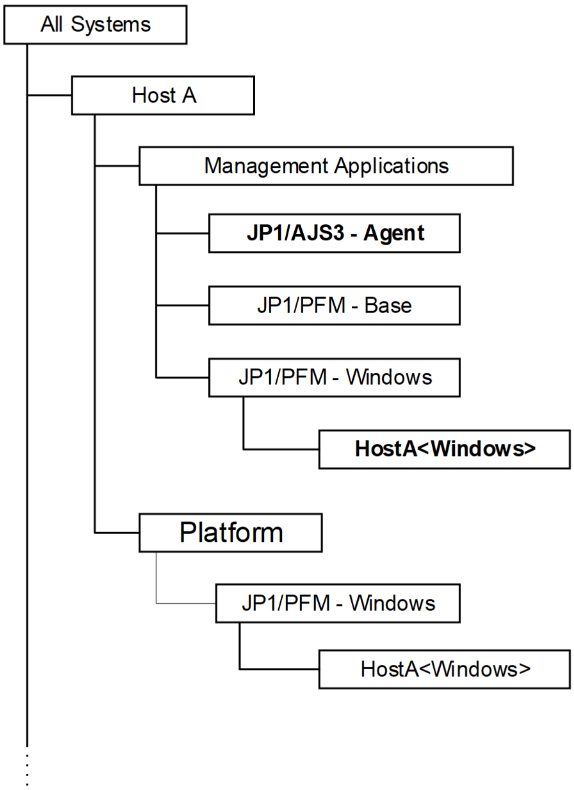
Suggestion display criteria

- Suggestions are displayed on the JP1/PFM - Agent node to which health check events are mapped.
- The JP1 permission of JP1_AJS_Admin or JP1_AJS_Editor is granted to the user.
- Suggestion activation criteria
- The JP1/AJS - Agent node exists on the same host as the selected IM management node, to which a health check event indicating that the host stopped was issued within the past one hour, and the event status is now Unprocessed.

Response action

- Navigate the window to the **Related node** tab on the JP1/AJS - Agent that exists on the same host as the selected IM management node.

Figure 2‒2: Example of the tree structure when JP1/AJS - Agent and JP1/PFM - Agent exist on the same host



In the above figure, *JP1/AJS3 - Agent* represents the JP1/AJS - Agent node. The tree SID is as follows:

```
_ROOT_AllSystems/_HOST_HOSTA/_CATEGORY_managementApplications/_OBJECT_JP1AJS
AGT
```

In the above figure, *HostA<Windows>* represents the JP1/PFM - Agent node to which the health check event is mapped. The tree SID is as follows:

```
_ROOT_AllSystems/_HOST_HOSTA/_CATEGORY_managementApplications/_SUBCATEGORY_J
P1%2FPFM%20-%20Windows/_OBJECT_JP1PFM-ATA1HostAJP1AGENTSERVICE
```

The following shows the definition in the suggestion definition file:

```
{
  "meta":{
    "version":"1"
  },
  "suggestions":[
    {
      "suggestionId":"check_affected_rootJobnet",
      "label":"Impact on root jobnets affected by host going down",
      "node":"_CATEGORY_managementApplications.*_OBJECT_JP1PFM-A",
      "permissions":[
        ["JP1_AJS_Admin"],
        ["JP1_AJS_Editor"]
      ],
      "cases":[
        [
          {
            "type":"struct",
            "key":{
              "idType":"tree",
              "sid":"${../..:tree:sid:}/_OBJECT_JP1AJSAGT"
            },
            "ope":"EXIST",
            "val":true,
            "description":"A JP1/AJS - Agent node exists on the same host wh
ere the selected node (PFM - Agent) exists"
          },
          {
            "type":"event",
            "key":{
              "sid":"${.:tree:sid:}",
              "statusFilter":[20,30,40],
              "B.TIME":["${:time:-1.h.:}","${:time::}"],
              "B.ID":["00004860"],
              "REGEX_B.MESSAGE":"KAVL15022-E.*hcsstatus=Host Not Available",
              "E.@JP1IM_DEALT":[0]
            },
            "ope":"EXIST",
            "val":true,
            "description":"A JP1 event indicating that the host stopped has 
been issued"
          }
        ]
      ],
      "action":{
        "type":"jump",
        "params":{
          "url":"index?sid=${../..:tree:sid:URLENC}%2F%5FOBJECT%5FJP1AJSAGT&
view=tree&tab=relation&eou=1"
        },
        "description":"Move to the Related node tab displaying the JP1/AJS 
- Agent node"
      }
    }
  ]
}
```

Single sign-on mapping definition file (imdd_sso_mapping.properties)

Format

```
user-ID-for-the-OpenID-provider = JP1-user-name
user-ID-for-the-OpenID-provider = JP1-user-name
...
```

Files

`imdd_sso_mapping.properties`

`imdd_sso_mapping.properties.model` (model file of the single sign-on mapping definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/`

Description

This file defines the mapping between the name of the JP1 user used in the Intelligent Integrated Management Base and the name of the user registered in the OpenID provider.

When the definitions are applied

When the `jddupdatessomap` command is completed successfully, the settings in the single sign-on mapping definition file take effect in the Intelligent Integrated Management Base.

When the definitions are applied

When the `jddupdatessomap` command is completed successfully, the settings in the single sign-on mapping definition file take effect in the Intelligent Integrated Management Base.

Information that is specified

Save the single sign-on mapping definition file in UTF-8 format, with no byte order mark (BOM) added to it.

The single sign-on mapping definition file has the following rules:

- Comment lines start with `#` or `!`.
- The user ID for the OpenID provider and the JP1 user name are case-sensitive.

- If an invalid format is found in a line, processing continues, ignoring the line.
- When you specify multiples user IDs for the same OpenID provider, the last specified one is enabled.
- There is no upper limit on the number of definitions.
- If the definition is applied when the file has no valid property at all, the `KAJY52031-W` message is output and the applied single sign-on mapping definitions are cleared.

user-ID-for-the-OpenID-provider

Specify the user ID registered in the OpenID provider. It is mapped to the JP1 user name specified on the right side.

JP1-user-name

Specify the name of the JP1 user registered in the JP1/Base authentication server. It is mapped to the user ID registered in the OpenID provider specified on the left side.

For details about the characters available in the JP1 user name, see the *JP1/Base User's Guide*.

The JP1 user requires the JP1 permission level of `JP1_Console_Admin`, `JP1_Console_Operator`, or `JP1_Console_User`, which is needed to log in to the Intelligent Integrated Management Base. If an unregistered JP1 user or a JP1 user without the JP1 permission is specified, the `KAJY52027-E` error occurs upon user authentication.

DS users whose JP1 authentication information is managed in the directory server through directory server linkage of JP1/Base are not applicable for single sign-on mapping authentication. If a DS user goes through authentication when the user is specified in the single sign-on mapping definition file, the `KAJY52027-E` error occurs during user authentication. For details about directory server linkage of JP1/Base, see the *JP1/Base User's Guide*.

Notes

- The user ID for the OpenID provider contains all characters, except for the end-of-line symbol, from the first non-space character to before the first unescaped =, `:`, or a space character.
- If you use characters that show the end of the user ID for the OpenID provider (=, `:`, or a space character) in the user ID, add a backslash before the end-indicating character to escape it.
- If you use characters that show the comment at the beginning of the user ID for the OpenID provider (`#` or `!`) in the user ID, add a backslash before the comment-indicating character to escape it.

The following table lists characters that must be escaped when used in the user ID for the OpenID provider.

Table 2–11: Characters that must be escaped when used in the user ID for the OpenID provider

No.	Character	Unicode	When it must be escaped
1	=	`\u003D`	Always required
2	:	`\u003A`	
3	Space	`\u0020`	
4	#	`\u0023`	Required for the first character
5	!	`\u0021`	

Example definition

```
OpenIDuser001 = JP1admin
OpenIDuser002 = JP1ope
...
```

Auto response action definition file (autoactconf.json)

Format

Same as *7.2.4(1) Auto Response Action definition Object*.

The file size limit is 10MB.

Files

`autoactconf.json`

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\responseaction`

For a logical host:

shared-folder`\jp1imm\conf\imdd\responseaction`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/responseaction`

For a logical host:

shared-directory`/jp1imm/conf/imdd/responseaction`

Character code

UTF-8 (If file has a BOM, load it ignoring BOM)

Description

A file that restores execution conditions in automatic response action and automatic response action definition, which is executed contents are recorded

When the definitions are applied

When JP1/IM - Manager service is started or auto response action definition file import command (jddupdateaction) is executed, this file is imported and applied to the system.

Information that is specified

Same as *7.2.4(1) Auto Response Action definition Object*.

Example definition

Same as *7.2.4(1) Auto Response Action definition Object*.

Response action state monitoring definition file (responseactionnotice.conf)

Format

```
{
    "meta":{
        "version":"version-information",
    },
    "eventnotice":{
        "autoactionevent":"[automatically-notify-response-action-status]",
    }
}
```

Files

`responseactionnotice.conf`

`responseactionnotice.conf.model` (model file of the response action state monitoring definition file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\responseaction`

For a logical host:

shared-folder`\jp1imm\conf\imdd\response action`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/responseaction`

For a logical host:

shared-directory`/jp1imm/conf/imdd/responseaction`

Character code

This file should be saved in UTF-8 without being granted BOM (byte order mark).

Description

A file that defines setup for monitoring execute status for automated response action.

When the definitions are applied

Turns enable when JP1/IM - Manager starts.

Information that is specified

The following table lists the members that can be specified:

Member		Data type	Description	Remarks
meta		object	Setup of the meta-information.	Required
	version	string	Specifies version of response action state monitoring definition file. Specify 1 as the fixed value.	Required
eventnotice		object	Setup to notify the event when status is changed.	Optional
	autoactionevent	string[]	Specifies status for auto response action to be notified when it reaches which status. You can specify one of the following: • SENDED Issues a JP1 event when sending request of response action execute to JP1/IM - Manager managing JP1/IM agent control base to run was completed (when response action's status changes to "Execute control sending"). • RUNNING Issues a JP1 event when sending request of response action execute to JP1/IM agent control base to run was completed (when status of response action is "Queuing"). • ENDED Issues a JP1 event when the command Execute in JP1/IM agent control base is completed (when status in response action is "Terminated" or "Forcibly killed" or "Canceled"). • ERROR A JP1 event is issued when Status of Response Action becomes an abnormal Status (when status of response action becomes "Fail," "Communication failed," or "Execute failed"). This member can have more than one setup. The defaults (default value, assuming an error occurs) work with Status that does not have this member setup.	Optional

Example definition

The following is a sample definition for issuing a JP1 event when execute of auto response action terminates or an execution fails.

```
{
    "meta":{
        "version":"1"
    },
    "eventnotice":{
        "autoactionevent":["ENDED","ERROR"]
    }
}
```

User-created definition file list definition file (imdd_user_deffile_list.json)

Format

- Format of the definition file

```
{
  "filelist":[
    {
      "filename": "filename",
      "filepath": "full-path-of-file",
      "filecategoryID": "category-ID-of-file",
      "filecategoryName": "category-name-of-file",
      "updateaction": "manipulation-for-definition-import"
    }, ...
  ]
}
```

- Format of the model file

```
{
  "filelist":[
    {
      "filename": "",
      "filepath": "",
      "filecategoryID": "",
      "filecategoryName": "",
      "updateaction": ""
    }
  ]
}
```

Files

`imdd_user_deffile_list.json`

`imdd_user_deffile_list.json.model` (model file)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imdd\fileoperation\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\fileoperation\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/fileoperation/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/fileoperation/`

Description

A file that defines a user-created file that can be updated or delete with the functions provided by JP1/IM - Manager.

When the definitions are applied

Reflected when definition file list acquisition API is executed.

Character code

UTF-8 (If file has a BOM, load it ignoring BOM)

Information that is specified

Item name	Optiona l	Description
filename	No	Indicates file name.
filepath	Yes	Destination of file is written in absolute path. If file path (absolute path including file name) exceeds 200 characters, it becomes error. If file with the name specified in filename does not exist in the specified file path, it is regarded as an invalid definition. If this setup field is omitted, "*manager-path*`\conf\imdd\user`" is assumed. (For logical environments, replace "*manager-path*" with "*shared-folder*`\jp1imm`".)
filecategoryID	Yes	Describes the category ID to be specified when grouping more than one file. A file with the same category ID is considered to belong to the same category. Allowed characters are alphanumeric characters, "`-`" (hyphen), and "`_`" (underscore). Up to 32 characters can be specified. Category ID starting with "`jp1_`" cannot be specified.
filecategoryName	Yes	Specifies the category name for category ID. Specify a character other than a control character. Up to 32 characters can be specified. If no `filecategoryID` is specified, this setup field is ignored. If a `filecategoryID` is specified and this setup field is not specified, `filecategoryID`'s value is setup.
updateaction	Yes	Describes the action (command-line) that should be executed if file is updated. For detail, see ■*Description of updateaction*.

■Description of `updateaction`

You can list the commands that Execute after updating file. The maximum length of a command line that can be written is 4,096 bytes.

If execute destination is a 64-bit Windows and you specify commands that are located in the `%WINDIR%\System32` folders or lower, be aware of WOW64 redirection function.

The following types of commands can execute:

Hosts that execute commands are Windows

- Execution format file (`.com`, `.exe`)
- Batch file (`.bat`)
- The scripting file of JP1/Script (`.spt`) (but the association must be setup so that `.spt` file can execute)

Hosts that execute commands are Linux

- Linux commands
- Shell scripts

Note that you cannot execute the following commands:

- Commands that require interaction
- Commands to display the screen
- Commands with escape sequences or control codes
- Commands that do not terminate, such as daemons
- Commands that require interaction with the desktop, such as Windows Message functions and DDE (in Windows)
- Commands that shutdown OS, such as `shutdown` or `halt`

■About files that can be specified for user-created definition file list definition file

File that can be described in user-created definition file list definition file is shown below.

- User-created suggestion definition file (`imdd_suggestion_`*any-file-name*`.conf`)
- Correlated Event Publishing Definition File
- Correlated event publishing environment-definition File
- Definition file for extended event attributes
- Definition file for extended event attributes (extended file)
- Common exclusion conditions Extended Definition File
- Definition file for opening monitor windows
- User-specific metric definition file (`metrics_`*any-Prometheus-trend-name*`.conf`)

When `jco_spmd_reload` command is specified in updateaction for update of definition file of JP1/IM3 - Manager in logical host environment, `-h` option is not needed.

■About user-created definition file, which output destination is as you want

For the definition file that you create, if files can specify any location as the storage destination, when using the definition file manipulation function, the definition file is stored must be in as follows:

In Windows

For a physical host:

Manager-path`\conf\imdd\user\`

For a logical host:

shared-folder`\jp1imm\conf\imdd\user\`

In UNIX

For a physical host:

`/etc/opt/jp1imm/conf/imdd/user/`

For a logical host:

shared-directory`/jp1imm/conf/imdd/user/`

Example definition

```
{
  "filelist":[
    {
      "filename": "file_def.conf",
      "filepath": "C:\\Program Files (x86)\\Hitachi\\JP1IMM\\conf\\imdd\\use
r",
      "filecategoryID": "user_def",
      "filecategoryName": "user_def",
      "updateaction": "JP1Cons\\bin\\jco_spmd_reload.exe"
    }
  ]
}
```

Definition file properties file (imdd_file_properties.json)

Format

```
{
  "filelist":[
    {
      "filename": "filename",
      "filepath": "full-path-of-file",
      "updateaction": "manipulation-for-definition-import",
      "message": "message"
    }, ...
  ]
}
```

Files

`imdd_file_properties.json`

Storage directory

Place the definition file that you want to work with in the get or refresh functions of the definition file into the compressed zip file.

Description

This file describes file name, file path, and file import operations for the definition file that are to be manipulated by the acquisition or update functions of the definition file.

When the definitions are applied

None

Information that is specified

Item name	Description
filename	Indicates File.
filepath	Destination of file is written in absolute path. If file path (absolute path including File name) exceeds 200 characters, it becomes error.
updateaction	For Windows, describe the action (command-line) to execute when the definition file is updated at the file destination directory that is the relative path from one layer upper from installed directory. For Linux, describe the action (command-line) to execute when the definition file is updated at the relative path from `/opt/`. For details, see the section ■*Description of updateaction* in *User-created definition file list definition file (imdd_user_deffile_list.json)*.
message	Returns the error message ID and its message body. If it succeeds, omit this item.

Character code

UTF-8 (If file has a BOM, load it ignoring BOM)

Example definition

```
{
  "filelist":[
    {
      "filename": "file_def.conf",
      "filepath": "C:\\Program Files (x86)\\Hitachi\\JP1IMM\\conf\\imdd\\use
r",
      "updateaction": "JP1Cons\\bin\\jco_spmd_reload.exe"
    }
  ]
}
```

Event-source-host mapping definition file (user_hostmap.conf)

Format

```
[DESC_VERSION=version-information]
#Comment
def definition-name-1
    cnd
        event-condition
    end-cnd
    source_attr attribute-name
end-def
def definition-name-2
    cnd
        event-condition
    end-cnd
    source_attr attribute-name
end-def
```

File

`user_hostmap.conf` (Event-source-host mapping definition file)

`user_hostmap.conf.model` (model file for the event-source-host mapping definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\hostmap\`

For a logical host:

shared-folder`\jp1cons\conf\hostmap\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/hostmap/`

For a logical host:

shared-directory`/jp1cons/conf/hostmap/`

Description

This file defines the conditions and the mapping source for a JP1 event to which the event source host is mapped by using the event source host mapping function. The maximum size of the event-source-host mapping definition file is 17 megabytes.

The event source host mapping function maps the event source host for the JP1 event that matches the event condition according to the definition in this file.

When the definitions are applied

The definition takes effect when the event source host mapping function is enabled and either of the following conditions is satisfied:

- JP1/IM is running
- The `jco_spmd_reload` command is executed

Information that is specified

`DESC_VERSION=`*version-information*

Specify `1`, which is the file version of the event-source-host mapping definition file. Specify `DESC_VERSION` on the first line of the definition file (the first line in the file that is not a null line or a comment line). If there is no file version on the first line, `1` is assumed as the file version.

`#` *comment*

Provides an explanation of the event-source-host mapping definition file.

`def` to `end-def`

These parameters mark the start and end of the mapping definition block. The block from `def` to `end-def` can be omitted.

After `def` comes the definition name of the event source host mapping definition. If you specify `def`△△△*definition-1*△△△*definition-2*△△△, then △△*definition-1*△△△*definition-2*△△△ are treated as the definition names (Δ indicates a single-byte space).

Each definition name must be unique within the event-source-host mapping definition file. The length of a character string is from 1 to 50 bytes.

Permitted characters are all characters other than control characters.

The control characters are ASCII `0x00` to `0x1F` and `0x7F` to `0x9F`.

`cnd` to `end-cnd`

These parameters mark the start and the end of the block that specifies conditions for the JP1 events to be mapped. You must specify one event condition block in a mapping definition block. The event condition block cannot be omitted. If a received JP1 event satisfies multiple event conditions, the definition block closest to the beginning of the event-source-host mapping definition file takes precedence. Tabs and spaces before and after the `cnd` and `end-cnd` parameters are ignored.

event-condition

Specifies conditions for the JP1 event to be mapped. You can specify from 1 to 256 event conditions for each event condition block. Event conditions are connected with the AND condition. Specify an event condition in the following format:

attribute-name comparison-keyword operand

attribute-name

Specifies the name of the attribute you want to compare. To specify a basic attribute, prefix the name with `B.`. To specify an extended attribute (common information or user-specific information), prefix the name with `E.`. The attribute name is case sensitive.

The following table lists and describes the combinations of attribute names and comparison keywords and the operands that can be specified.

Table 2–12: Combinations of attribute names and comparison keywords and the operands that can be specified

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	`B.ID`	• `Match` • `Do not match`	A maximum of 100 event IDs can be specified. Specify event IDs in hexadecimal notation. Event IDs are not case sensitive. The permitted range is from `0` to `7FFFFFFF`.

No.	Item	Attribute name	Comparison keyword	Operand
2	Reason for registration	B.REASON	• Match • Do not match	A maximum of 100 reasons can be specified.
3	Source process ID	B.PROCESSID	• Match • Do not match	A maximum of 100 source process IDs can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
4	Source user ID	B.USERID	• Match • Do not match	A maximum of 100 source user IDs can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
5	Source group ID	B.GROUPID	• Match • Do not match	A maximum of 100 source group IDs can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
6	Source user name	B.USERNAME	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 source user names can be specified. However, if a regular expression is used, only one source user name is allowed.
7	Source group name	B.GROUPNAME	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 source group names can be specified. However, if a regular expression is used, only one source group name is allowed.
8	Event-issuing server name (source host)#	B.SOURCESERVER	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 event-issuing server names can be specified. However, if a regular expression is used, only one event-issuing server name is allowed.
9	Target event server name#	B.DESTSERVER	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 target event server names can be specified. However, if a regular expression is used, only one target event server name is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
10	Message	`B.MESSAGE`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 messages can be specified. However, if a regular expression is used, only one message is allowed.
11	Event level	`E.SEVERITY`	• `Match`	Multiple event levels can be specified. If multiple event levels are specified, the same event level cannot be specified twice. However, if a regular expression is used, only one event level is allowed. The following values can be specified: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, or `Debug`
12	User name	`E.USER_NAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 user names can be specified. However, if a regular expression is used, only one user name is allowed.
13	Product name	`E.PRODUCT_NAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 product names can be specified. However, if a regular expression is used, only one product name is allowed.
14	Object type	`E.OBJECT_TYPE`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 object types can be specified. However, if a regular expression is used, only one object type is allowed.
15	Object name	`E.OBJECT_NAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained`	A maximum of 100 object names can be specified. However, if a regular expression is used, only one object name is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• Regular expression	
16	Root object type	E.ROOT_OBJECT_TYPE	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 root object types can be specified. However, if a regular expression is used, only one root object type is allowed.
17	Root object name	E.ROOT_OBJECT_NAME	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 root object names can be specified. However, if a regular expression is used, only one root object name is allowed.
18	Object ID	E.OBJECT_ID	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 object IDs can be specified. However, if a regular expression is used, only one object ID is allowed.
19	Occurrence	E.OCCURRENCE	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 occurrences can be specified. However, if a regular expression is used, only one occurrence is allowed.
20	Return code	E.RESULT_CODE	• First characters • Match • Do not match • Is contained • Is not contained • Regular expression	A maximum of 100 return codes can be specified. However, if a regular expression is used, only one return code is allowed.
21	Program-specific extended attribute	E.*xxxxxxx*	• First characters • Match	For the attribute name, you can specify a character string with a maximum of 32 bytes that begins with an uppercase letter

No.	Item	Attribute name	Comparison keyword	Operand
			- Do not match - Is contained - Is not contained - Regular expression	and consists of uppercase letters, numeric characters, and the underscore (_). A maximum of 100 program-specific extended attributes can be specified. However, if a regular expression is used, only one program-specific extended attribute is allowed.

#

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is `Match` or `Do not match`, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than `Match` or `Do not match` is selected, a business group name specified in a path format is treated as a host name.

If the `-ignorecasehost` option of the `jcoimdef` command is set to `ON` and a comparison keyword other than `Regular expression` is selected, the character string is no longer case sensitive.

comparison-keyword

Specifies `BEGIN` (begins with), `IN` (matches), `NOTIN` (does not match), `SUBSTR` (includes), `NOTSUBSTR` (does not include), or `REGEX` (regular expression) as the comparison keyword. The comparison keyword is case sensitive.

operand

Specifies a character string as the value that is to be compared with the attribute value specified for the comparison keyword. The operand is case sensitive.

If you specify two or more operands, separate them by one or more consecutive spaces or tabs. The OR condition is applied to the specified operands. Note that if a regular expression is specified, only one operand is allowed.

If you want to a space or a tab as part of an operand, use the format shown in the following table.

No.	Value to be specified	How to specify
1	Tab (`0x09`)	`%09`
2	Space (`0x20`)	`%20`
3	`%` (`0x25`)	`%25`
4	CR (`0x0d`)	`%0d`
5	LF (`0x0a`)	`%0a`

During maximum value checking of the definition format, `%20` and `%25` are each treated as a single character. The following shows an example of defining ID matches `100` and `200`, which selects multiple operands:

```
B.IDΔINΔ100Δ200
```

Legend: Δ indicates a single-byte space (`0x20`)

You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length in bytes of all operands that are specified in the event condition block).

`source_attr`

Specifies the attribute value of the mapping source. For `source_attr`, you can specify a value that stores the event source host name. This parameter cannot be omitted. Specify the `source_attr` in the following format:

`source_attr` *mapping-source-attribute-value*

You can specify an attribute name or a variable name for the mapping source attribute value. If you specify an attribute name, all information related to the attribute value is stored. If you specify a variable name, part of an attribute value is extracted (partial extraction) and stored.

The attribute you can specify for the mapping source attribute value is an extended attribute (program-specific information). Extended attributes (program-specific information) are attributes that are not included in the common information described in *Table 3-2 List of common information provided by extended attributes*. You can specify `$EVENV1` to `$EVENV9` for the variable name.

Example definition

The following example shows how to set the host name (`AGENT_A`) contained in a message as the event source host name when the event ID is `100`, the event level is `Warning`, and the message is `An error with error code 1111 occurred on the AGENT_A host.` (where `AGENT_A` is a host name):

```
DESC_VERSION=1
#Maps the host name in the message to the event source host name.
def event-source-host-mapping-1
    cnd
        B.ID IN 100
        E.SEVERITY IN Warning
        B.MESSAGE REGEX An error occurred on the host ([a-zA-Z0-9\-_]+) wit
h error code 1111.
    end-cnd
    source_attr $EVENV1
end-def
```

Automated action environment definition file (action.conf.update)

Format

```
[logical-host-name\JP1CONSOLEMANAGER\ACTION]
"ACTIONINFSIZE"=dword:hexadecimal-value
"EVENTALIVEPERIOD"=dword:hexadecimal-value
"ACTIONEXECUSER"="JP1-user-name"
"ACTIONDEFFILE"="file-name"
"HOSTINEVENT"="{remote | local}"
"ACTIONINFFILE"="file-name"
"ACTIONLIMIT"=dword:hexadecimal-value
"SENDABLE_EVENT"="event-ID"
"REGEXP"="{JP1|EXTENDED}"
"ACTIONPRIORITY"="{DEFAULT|V8COMPATIBLE}"

[logical-host-name\JP1CONSOLEMANAGER\LOG_CONTROL\JCAMAIN]
"LOGSIZE"=dword:hexadecimal-value
```

This is the format of the parameters in the common definition information. Do not edit any other parameters because they are used internally.

File

`action.conf.update` (model file for the automated action environment definition file)

Storage directory

In Windows

Console-path`\default\`

In UNIX

`/etc/opt/jp1cons/default/`

Description

This file defines an execution environment for automated actions.

The required definitions are provided as a model file. To change the settings, copy the model file and edit the copy after renaming the copy to definition file (for Windows: *console-path*`\conf\action.conf`, for UNIX: `/etc/opt/jp1cons/conf/action.conf`).

To reduce the size of the action information file

Make a backup of the action information file, delete the action information file, and then change the settings.

When the definitions are applied

The specified definitions take effect when JP1/IM - Manager starts after you have executed the `jbssetcnf` command to apply the definitions to the JP1 common definition information.

You can also apply the following parameters by reloading them with the `jco_spmd_reload` command:

- `EVENTALIVEPERIOD`
- `ACTIONEXECUSER`

- `HOSTINEVENT`
- `SENDABLE_EVENT`

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER\ACTION]`

Specifies a key name for the action execution environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for a physical host and *logical-host-name* for a logical host.

`"ACTIONINFSIZE"=dword:`*hexadecimal-value*

Specifies the size of the action information file as a hexadecimal value (kilobytes).

The permitted value is from `dword:00000001` to `dword:00001000` (1 to 4,096 kilobytes). The default value is `dword:00001000` (4,096 kilobytes).

The action information file stores automated action execution information. The file is referenced when an action is referenced from the event console or by the `jcashowa` command as well as when an action status notification event is issued.

This is a wrap-around file that is overwritten when the specified `ACTIONINFSIZE` value is reached. Once overwritten, old action information might no longer be viewable in the event console or with the `jcashowa` command and action status notification events might no longer be issued. If you will reference past action execution results or issue action information notification events, you must estimate the size of the action information that you will want to reference and then set that value in `ACTIONINFSIZE`.

For details about how to estimate the size of the action information file, see the Release Notes for JP1/IM - Manager.

When you set the action information file size to the default value, you can reference information equivalent to 65,535 actions.

`"EVENTALIVEPERIOD"=dword:`*hexadecimal-value*

Specifies the AND event storage period in minutes.

The permitted value is from 1 to 1,440 (minutes), expressed as a hexadecimal value. The default is `dword:0000003c` (60 minutes).

`"ACTIONEXECUSER"="`*JP1-user-name*`"`

Specifies a JP1 user as the default user who executes actions.

Express the JP1 user as a character string of no more than 15 bytes. The default is `""` (none). If this parameter is omitted, `jp1admin` is assumed.

When no execution user is specified in an automated action definition, the action will be executed by the JP1 user defined here.

`"ACTIONDEFFILE"="`*file-name*`"`

Specifies a name for the automated action definition file.

The default is `actdef.conf`; you cannot change this default value.

Use this automated action definition file to define conditions for executing actions by the automated action function and the commands to be executed.

`"HOSTINEVENT"="{`<u>`remote`</u>` | local}"`

Specifies the method to be used to acquire the host name at the event source.

The permitted values are `remote` and `local`. The default is `remote`.

- When `remote` is set, the event attribute *event-issuing server name* is used as the event source host name.
- When `local` is specified, if the source IP address in the event attribute is an IPv6 address in JP1/IM - Manager, the host name found by using `getnameinfo` is used as the event source host name. If, however, the source IP

address is an IPv4 address, the host name found by using `gethostbyaddr` is used as the event source host name. If the host name cannot be found, the IP address is used as the event source host name.

Note:

If `"local"` is specified, the action matching might take a longer time due to DNS queries or other reasons.

`"ACTIONINFFILE"="`*file-name*`"`

Specifies a name for the action information file.

The default is `actinf.log`. You cannot change this default value.

`"ACTIONLIMIT"=dword:`*hexadecimal-value*

Specifies the number of commands to be pre-loaded.

If you use JP1/Base version 06-51 or earlier at the automated action execution host, specify the number of commands that are to be pre-loaded at the execution host. The permitted value is from `dword:00000001` to `dword:00000040` (1 to 64). The default is `dword:0000000a` (10).

If you use JP1/Base version 06-71 or later at the automated action execution host, set the number of pre-loaded commands in JP1/Base at the execution host. In this case, use the `jcocmddef` command at the execution host to set the number of pre-loaded commands. The default is 1,024 commands.

For details, see *14.7.6 Command execution environment* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`"SENDABLE_EVENT"="`*event-ID*`"`

Specifies an automated action issuance event (JP1 event whose event ID is `20A0`, `20A1`, `20A2`, `20A3`, or `20A4`).

The permitted values are `20A0`, `20A1`, `20A2`, `20A3`, and `20A4`. To specify multiple event IDs, separate them with the space.

The default is `"20A0 20A3 20A4"`.

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

`"REGEXP"="{JP1|`<u>`EXTENDED`</u>`}"`

Specifies the type of regular expressions to be used.

The permitted values are `JP1` and `EXTENDED`. The default is `EXTENDED`.

If you specify `JP1`, you can use JP1-specific regular expressions to define automated actions. If you specify `EXTENDED`, you can use extended regular expressions to define automated actions.

Note that this parameter is used only for Windows, and is not necessary for UNIX.

`"ACTIONPRIORITY"="{DEFAULT|`<u>`V8COMPATIBLE`</u>`}"`

Specifies the priority order for actions.

The permitted values are `DEFAULT` and `V8COMPATIBLE`. These values are case sensitive.

If this parameter is omitted altogether, `V8COMPATIBLE` is assumed.

When JP1/IM - Manager is initially installed, `DEFAULT` is set.

When JP1/IM - Manager is upgraded from version 8 or earlier, the `ACTIONPRIORITY` parameter is not set.

- If `DEFAULT` is specified and multiple action definitions are specified for the same parameter, the first action definition specified in the automated action definition file takes effect.

- If `V8COMPATIBLE` is specified, the same priority order is applied as is used for the automated action function in JP1/IM - Manager versions earlier than 09-00. In other words, if multiple action definitions are specified for the same parameter, an action definition with an event ID specified takes precedence over an action definition for all events, and an action definition with an event ID that is specified closest to the beginning of the automated action definition file takes precedence over all other action definitions with event IDs specified.

`[`*logical-host-name*`\JP1CONSOLEMANAGER\LOG_CONTROL\JCAMAIN]`

Specifies a key name for the automated action log definition.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"LOGSIZE"=dword:`*hexadecimal-value*

Specifies the maximum size of an automated action trace log (1 file).

The permitted value is from 65,536 to 104,857,600 bytes (64 kilobytes to 100 megabytes), expressed in bytes as a hexadecimal value. The default is `dword:00500000` (5,242,880 bytes (5 megabytes)).

The default value will not cause wrap-around in the file even when 300 commands with a maximum length of 100 bytes per command are executed for actions. To change the log size, see the Release Notes for JP1/IM - Manager and then estimate the log size.

Example definition

```
[JP1_DEFAULT\JP1CONSOLEMANAGER\ACTION]
"ACTIONINFSIZE"=dword:00001000
"EVENTALIVEPERIOD"=dword:0000003c
"ACTIONEXECUSER"="JP1USER"
"ACTIONDEFFILE"="actdef.conf"
"HOSTINEVENT"="remote"
"ACTIONINFFILE"="actinf.log"
"SENDABLE_EVENT"="20A0 20A3 20A4"
"REGEXP"="JP1"

[JP1_DEFAULT\JP1CONSOLEMANAGER\LOG_CONTROL\JCAMAIN]
"LOGSIZE"=dword:00100000
```

Make sure that the end of the file is at the beginning of the last line.

Automated action definition file (actdef.conf)

Format

```
[#automated-action-definition-file-version]
[DESC_VERSION=version-information]

[#automated-action-status-monitoring-parameter]
cmn
    [sta {true|false}]
end-cmn

[#automated-action-definition-parameter]
act action-name
    [prm parameter-group]
    [cmt comment]
    aid action-ID
    [valid true|false]
    eid event-ID

    cnd
        event-conditions
    end-cnd

    [usr user-name]
    [hst {execution-host-name|group-name|business-group-name|monitoring-grou
p-name}]
    [cmd action]
    [var environment-variable-file-name]

    [det suppress-period]
    [ret delay-monitoring-period]
end-act
```

File

`actdef.conf` (automated action definition file)

`actdef.conf.model` (model file for the automated action definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\action\`

For a logical host:

shared-folder`\jp1cons\conf\action\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/action/`

For a logical host:

shared-directory`/jp1cons/conf/action/`

Description

This file defines conditions for executing actions by the automated action function of JP1/IM and the commands to be executed as the actions. To use the language encoding that is used by JP1/IM - Manager, specify this file.

The maximum size of an automated action definition file is 22 megabytes (23,068,672 bytes).

The automated action function automatically executes a specified command on the basis of the definition specified in this file when a JP1 event satisfying specified conditions is received.

Each line of action definition information is called a *parameter*. There are three types of parameters in an automated action definition file:

- Automated action definition file version
  Defines the format version of the automated action definition file.
- Automated action status monitoring parameter (common block)
  Specify the `cmn` parameter in the common block to define whether the status of automated actions is to be monitored.
- Automated action definition parameters (action block)
  Specify parameters, such as `prm` and `cmt`, in the action block to define conditions for executing an action and the command to be executed as the action.

You must specify the automated action definition file version and the automated action status monitoring parameter before the automated action definition parameters. If you specify the automated action definition file version and/or the automated action status monitoring parameter after the automated action definition parameters, the specified definition is ignored.

If you specify the automated action definition file version or the automated action status monitoring parameter more than once, the first definition specified takes effect and subsequent definitions are ignored.

Definition specification

- Use the space or the tab to separate the words in a parameter.
- Any space or tab character at the beginning or at the end of a line is ignored.
- A line beginning with hash mark (`#`) is regarded as a comment except when the hash mark (`#`) is preceded by a character string.
- Use lowercase letters to specify the parameter names in action definitions. A specified parameter name that contains uppercase letters is treated as being invalid and results in a definition error.

Action priority

If a received JP1 event satisfies the execution conditions in multiple automated action definitions, only the automated action that has the highest priority is executed (for each parameter group discussed below). The automated action priority order is determined by the following rule:

- The first action specified in the automated action definition file (in GUI, the first action displayed in the Action Parameter Definitions) takes precedence over the other actions.

You can change the action priority order in the common definition. For details about the priority order of automated actions, see *6.3.2 Precedence of execution conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Parameter groups and AND conditions

Each automated action definition parameter belongs to a *parameter group*. A parameter group is a unit for checking the conditions for executing an automated action. Use of parameter groups enables you to specify complex conditions, such as when multiple actions are to be executed for a single JP1 event or when an action is to be executed only when multiple conditions are satisfied.

When a single JP1 event arrives at the manager host of JP1/IM, the automated action definition parameters and execution conditions are compared for each parameter group in order of priority. When execution conditions that are satisfied are found, only the automated action definition parameter that has the highest priority is executed for each parameter group.

If you specify an ampersand (`&`) in a parameter group, an AND condition with the automated action definition parameter defined on the preceding line is created. When automated action definition parameters are specified in an AND condition, the corresponding action is executed when all the conditions are satisfied.

Checking the specified information

Use the `jcamakea` command to check the information specified in the definition file.

When the definitions are applied

The definition of an automated action takes effect when you click the **Apply** button in the Action Parameter Definitions window in JP1/IM - View when JP1/IM - Manager starts, or when you execute the `jcachange` command.

If you want to execute the `jcachange` command to re-load the definition, execute the `jcamakea` command first to make sure there are no errors in the definition.

Information that is specified (automated action definition file version)

This subsection describes the information to be specified as the automated action definition file version.

`DESC_VERSION=`*version-information*

Defines the format version of the automated action definition file. Specify this definition on the first line of the automated action definition file (the first line in the file excluding null lines and comment lines). If this information is specified on a line other than the first line, a definition error results.

Table 2–13: Automated action definition file format version information

Version information	Description
1	Automated action definition file version is 07-11 to 07-51.
2	Automated action definition file version is 08-01 to 08-50.
3	Automated action definition file version is 09-00 to 11-10.
4	Automated action definition file version is 11-50 or later.

If this parameter is omitted or 1 is specified, the value 2 is assumed for reading the file. When the **Apply** button is clicked in the Action Parameter Definitions window in JP1/IM - View, the value 2 is set.

If a value other than 1, 2, 3, or 4 is specified in this parameter, an error is output to the integrated trace log and the value 3 is assumed as the version information for reading the file.

In such a case, the Action Parameter Definitions window cannot be displayed in JP1/IM - View. To change the version information, directly edit the definition file.

Because the format of an old automated action definition file version is compatible with the automated action definition file format for version 08-01 or later, the format for version 08-01 or later is assumed for reading the file.

If this parameter is specified on a line that is subsequent to a line containing an automated action definition parameter, the Action Parameter Definitions window can no longer be displayed in JP1/IM - View.

Use the `jcamakea` command to check the contents of the automated action definition file.

Information that is specified (automated action status monitoring parameter)

This subsection describes the information to be specified in the automated action status monitoring parameter.

`cmn` to `end-cmn`

These are the start and end parameters for the block that specifies a parameter that is applicable to all action definitions. The portion between `cmn` and `end-cmn` is called a common block. This block must be specified before the automated action definition parameters. Specify this parameter only once in the automated action definition file. Specification of this block is optional. If this block is omitted, `false` is assumed for the `sta` parameter. The AND condition is applied to each event condition.

`sta {true|false}`

Specifies whether the action status is to be monitored.

Specify either `true` or `false`. To monitor the action status, specify `true`. To not monitor the action status, specify `false`. The default is `false`.

Information that is specified (automated action definition parameters)

This subsection describes each item that is specified in the automated action definition parameters.

`act` *action-name* to `end-act`

Specifies the start and end parameters of an automated action definition. There is no limit to the number of actions that can be defined between `act` and `end-act`; however, at least one action must be specified. The portion between `act` *action-name* and `end-act` is called an action block.

After `act`, specify an action name, expressed using from 1 to 50 bytes of characters. The permitted characters are all characters other than the control characters (from `0x00` to `0x1F` and from `0x7F` to `0x9F`).

Each action name must be unique among the action names specified in all the action blocks. The parameters that can be specified in the action block are as follows:

`prm`, `cmt`, `eid`, `cnd` to `end-cnd`, `usr`, `hst`, `cmd`, `var`, `det`, `ret`, `aid`, `valid`

`prm` *parameter-group*

Specifies a number for the parameter group. If this parameter is omitted, `0` is assumed.

You can specify a single numeric digit (from 0 to 9) or the ampersand (`&`). If you specify a numeric digit, you cannot omit the action name. If you specify an ampersand (`&`), this parameter becomes part of an AND condition with the immediately preceding action block, which means that the automated action definition parameter in this action block belongs to the same parameter group as the immediately preceding action block. When an ampersand (`&`) is specified, the action name cannot be specified.

Following an action block for which the ampersand is not specified, you can specify a maximum of 9 action blocks as members of an AND condition (for a total of 10 action blocks including the first action block).

Within the same parameter group, the first action block specified (in the GUI, the top action block displayed in the Action Parameter Definitions window) has precedence over the other action blocks. When a JP1 event arrives at the manager, it is matched against the event conditions in the action block for each parameter group in the order of priority. When event conditions are found that match the JP1 event, the action in the action block that has the highest priority is executed for the parameter group and no more matching is performed for the action blocks that follow the executed action block. Events are matched in ascending order of parameter groups. For details about the priority order of automated actions, see *6.3.2 Precedence of execution conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`cmt` *comment*

Specifies a comment about the action block. This parameter is optional. Specify a comment using from 1 to 1,040 bytes of characters. All characters are permitted. If a comment exceeds 1,040 bytes in length, the portion in excess of 1,040 bytes is deleted.

`aid` *action-id*

Specifies the action ID. This parameter cannot be omitted. The action ID can be any number from 0 to 2,147,483,647. However, this parameter cannot be specified when you have specified `&` for the *parameter-group*.

This parameter can be specified only when the version information is 4.

`valid true|false`

Enables or disables (specifies `true` or `false`, respectively) the automated action definition. This parameter is optional. If this parameter is omitted, the value is assumed to be `true`. However, this parameter cannot be specified when you have specified `&` for the *parameter-group*. When you have specified `&` for the *parameter-group*, the status (enabled or disabled) of the automated action definition depends on the status of the previous action execution condition.

This parameter can be specified only when the version information is 4.

`eid` *event-ID*

Specifies the event ID for the action conditions. This parameter is mandatory and can be specified only once.

An event ID consists of a base part and an extension part. Express each part of an event ID as a string of from 1 to 8 hexadecimal characters, and separate the base part from the extension part with a colon (`:`). An event ID is not case sensitive. The extension part can be omitted. To specify any event ID, use an asterisk (`*`). When an asterisk is specified, all events become subject to the action. If JP1 events occur frequently, a large number of actions will be implemented, in which case execution may be delayed. When you specify an asterisk, you should narrow down the applicable events by using other conditions (such as a message, basic event information, detailed event information, and extended event information).

The following shows an example:

Example: Specify event ID A as follows:

```
eid a
eid A
eid 0000000a
eid 0000000A
eid 0000000A:0
eid 0000000A:00000000
```

Example: Specify any event ID as follows:

```
eid *
```

`cnd` *event-conditions* to `end-cnd`

Specifies the start and end parameters of the block that specifies event conditions for executing an action. Specification of an event condition block is mandatory. Specify only one event condition block within an action block. You can specify from 0 to 256 event conditions in an event condition block. The AND condition is applied to each event condition.

event-conditions

Specifies the event conditions in the following format (Δ indicates a single-byte space):

*attribute-name*Δ*comparison-keyword*Δ*operand*`[`Δ*operand*`]...`

Note that a line consisting of only spaces or tabs is ignored during processing.

attribute-name

Specifies the name of an attribute that you want to compare. To specify a basic attribute, place `B.` immediately before the name. To specify an extended attribute (common information or user-specific information), place `E.` immediately before the name. Attribute names are case sensitive.

comparison-keyword

Specifies one of BEGIN (begins with), IN (matches), NOTIN (does not match), SUBSTR (includes), NOTSUBSTR (does not include), or REGEX (regular expression) as the comparison keyword. The comparison keyword is case sensitive.

operand

Specifies a character string as the value that is to be compared with the attribute value by the specified comparison keyword. Operands are case sensitive.

To specify multiple operands, separate them with one or more consecutive spaces or a tab. The OR condition is applied to the specified operands. Note that when a regular expression is specified, only one operand can be specified.

To use a space, tab, end-of-line code (CR or LF), or % as part of an operand value, you must specify a value shown below:

No.	Value to be used	What to specify
1	Tab (0x09)	%09
2	Space (0x20)	%20
3	% (0x25)	%25
4	Linefeed code LF (0x0a)	%0a
5	Carriage return code CR (0x0d)	%0d

The character code specified after % is not case sensitive. When a JP1 regular expression is used, %0d cannot be specified. The following shows an example of defining ID matches 100 and 200, which selects multiple operands:

```
B.IDΔINΔ100Δ200
```

Legend: Δ indicates a single-byte space (0x20)

You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length in bytes of all operands that are specified in the event condition block).

Basic event information

If you specify B.BASIC as the attribute name, you can set the same conditions as for basic event information in the automated action definition file (for conversion).

When you specify B.BASIC as the attribute name, you must specify REGEX as the comparison keyword.

You can specify the operands in the same format as is used for basic event information in the automated action definition file (for conversion). Note that to use a space, tab, end-of-line code (CR or LF), or percent sign (%), specify %. Specify a forward slash (/) as /; there is no need to specify it as \/.

Detailed event information

If you specify B.DETAIL as the attribute name, you can set the same conditions as for detailed event information in the automated action definition file (for conversion).

When you specify B.DETAIL as the attribute name, you must specify REGEX as the comparison keyword.

You can specify the operands in the same format as is used for detailed event information in the automated action definition file (for conversion). Note that to use a space, tab, end-of-line code (CR or LF), or percent sign (%), specify %. Specify a forward slash (/) as /; there is no need to specify it as \/.

The following table lists and describes the attribute names, comparison keywords, and operands that can be specified in an event condition.

Table 2–14: Attribute names, comparison keywords, and operands that can be specified in an event condition

No.	Item	Attribute name	Comparison keywords	Operand
1	Event ID	`B.ID`	• `Match` • `Does not match` • `Regular expression`	Specifies an event ID. • A maximum of 100 event IDs can be specified. However, if a regular expression is used, only one event ID is allowed. • In the case of `Match` or `Does not match`, the event ID is not case sensitive. • The permitted range is from `0` to `7FFFFFFF`. • In the case of a regular expression, the event ID of an event to be compared is treated as having the following format: • When the extended part of the event ID is `0`: *basic-part-of-event-ID* (8-digit hexadecimal value consisting of uppercase letters and numbers) • When the extended part of the event ID is not `0`: *basic-part-of-event-ID* (8-digit hexadecimal value consisting of uppercase letters and numbers)`:`*extended-part-of-event-ID* (8-digit hexadecimal value consisting of uppercase letters and numbers) If the basic part or extended part of an event ID is a value that consists of fewer than 8 characters, leading 0s are added to obtain a string of 8 characters.
2	Source process ID	`B.PROCESSID`	• `Match` • `Does not match` • `Regular expression`	Specifies the process ID of the application program that issues the event. • A maximum of 100 source process IDs can be specified. However, if a regular expression is used, only one source process ID is allowed. • The permitted value range is from -2,147,483,648 to 2,147,483,647.
3	Registered time	`B.TIME`	`Regular expression`	Specifies the time the JP1 event was registered into the event database at the source host. • A regular expression in the format *YYYYMMDDhhmmss* must be used.
4	Arrived time	`B.ARRIVEDTIME`	`Regular expression`	Specifies the time the JP1 event arrived at the event database at the source host. • A regular expression in the format *YYYYMMDDhhmmss* must be used.

No.	Item	Attribute name	Comparison keywords	Operand
5	Source user ID	`B.USERID`	• `Match` • `Does not match` • `Regular expression`	Specifies the user ID (numeric value) of the source process. • A maximum of 100 source user IDs can be specified. However, if a regular expression is used, only one source user ID is allowed. • The permitted value range is from -2,147,483,648 to 2,147,483,647.
6	Source group ID	`B.GROUPID`	• `Match` • `Does not match` • `Regular expression`	Specifies the group ID (numeric value) of the source process. • A maximum of 100 source group IDs can be specified. However, if a regular expression is used, only one source user ID is allowed. • The permitted value range is from -2,147,483,648 to 2,147,483,647.
7	Source user name	`B.USERNAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the user name of the source process. • A maximum of 100 source user names can be specified. However, if a regular expression is used, only one source user name is allowed.
8	Source group name	`B.GROUPNAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the group name of the source process. • A maximum of 100 source group names can be specified. However, if a regular expression is used, only one source group name is allowed.
9	Source IP address	`B.SOURCEIPADDR`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the IP address of the event-issuing server. • A maximum of 100 source IP addresses can be specified. However, if a regular expression is used, only one source IP address is allowed. • To specify an IPv6 address, use a four-digit value in hexadecimal (`0` to `9` and `a` to `f`) as shown below. The alphabetic characters are case sensitive. Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff` • Lowercase letters cannot be changed to uppercase alphabetic characters, and IPv4-mapped address, IPv4-compatible addresses, and abbreviated IPv6 addresses cannot be specified.
10	Event-issuing server name (source host)#	`B.SOURCESERVER`	• `Match` • `Does not match` • `Is contained` • `Is not contained`	Specifies the host name of the host (event server name) where the JP1 event occurred. • A maximum of 100 event-issuing server names can be specified.

No.	Item	Attribute name	Comparison keywords	Operand
			• `First characters` • `Regular expression`	However, if a regular expression is used, only one event-issuing server name is allowed.
11	Message	`B.MESSAGE`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the message for a basic attribute of the event. • A maximum of 100 messages can be specified. However, if a regular expression is used, only one message is allowed.
12	Detailed event information	`B.DETAIL`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies detailed information for a basic attribute of the event. • A maximum of 100 detailed information items can be specified. However, if a regular expression is used, only one detailed information item is allowed. • If binary data is set in the detailed information for the JP1 event, the detailed information is treated as being the null character `""` (0 bytes) for performing comparison. • Available for compatibility purposes.
13	Reason for registration	`B.REASON`	• `Match` • `Does not match`	Specifies a reason for registration. • A maximum of 100 reasons for registration can be specified.
14	Start time	`E.START_TIME`	`Regular expression`	Specifies the execution start or restart time. • This item cannot be specified more than once. • Specify the absolute time in seconds using a regular expression.
15	End time	`E.END_TIME`	`Regular expression`	Specifies the execution end time. • This item cannot be specified more than once. • Specify the absolute time in seconds using a regular expression.
16	Product name	`E.PRODUCT_NAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the name of the product that issued the JP1 event. • A maximum of 100 product names can be specified. However, if a regular expression is used, only one product name is allowed.
17	Object type	`E.OBJECT_TYPE`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the type of object. • A maximum of 100 object types can be specified. However, if a regular expression is used, only one object type is allowed.

No.	Item	Attribute name	Comparison keywords	Operand
18	Object name	`E.OBJECT_NAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the object name of the JP1 event. • A maximum of 100 object names can be specified. However, if a regular expression is used, only one object name is allowed.
19	Root object type	`E.ROOT_OBJECT_TYPE`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the root object type of the JP1 event. • A maximum of 100 root object types can be specified. However, if a regular expression is used, only one root object type is allowed.
20	Root object name	`E.ROOT_OBJECT_NAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the root object name of the JP1 event. • A maximum of 100 root object names can be specified. However, if a regular expression is used, only one root object name is allowed.
21	Object ID	`E.OBJECT_ID`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the object ID of the JP1 event. • A maximum of 100 object IDs can be specified. However, if a regular expression is used, only one object ID is allowed.
22	Occurrence	`E.OCCURRENCE`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the occurrence of the JP1 event. • A maximum of 100 occurrences can be specified. However, if a regular expression is used, only one occurrence is allowed.
23	User name	`E.USER_NAME`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the user name of the user who issued the JP1 event. • A maximum of 100 user names can be specified. However, if a regular expression is used, only one user name allowed.
24	Result code	`E.RESULT_CODE`	• `Match` • `Does not match` • `Is contained` • `Is not contained` • `First characters` • `Regular expression`	Specifies the termination code. • A maximum of 100 termination codes can be specified. However, if a regular expression is used, only one termination code is allowed.
25	Severity	`E.SEVERITY`	• `Match` • `Regular expression`	Specifies the severity of the JP1 event. • The following severity levels can be specified: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`,

No.	Item	Attribute name	Comparison keywords	Operand
				Notice, Information, or Debug. - Multiple severity values can be specified. However, if a regular expression is used, only one severity value is allowed.
26	Event source host name#	E.JP1_SOURCEHOST	- First characters - Match - Does not match - Is contained - Is not contained - Regular expression	Specifies the event source host name of the JP1 event. - A maximum of 100 reasons for registration can be specified. However, if a regular expression is used, only one reason for registration is allowed.
27	Basic event information	B.BASIC	Regular expression	You can specify basic event information for compatibility with version 8 or earlier.
28	Program-specific extended attribute	--	- Match - Does not match - Is contained - Is not contained - First characters - Regular expression	Specifies the attribute name of a program-specific extended attribute. - You can specify a name with a maximum length of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_). - A maximum of 100 extended attribute names can be specified. However, if a regular expression is used, only one extended attribute name is allowed.

Legend:

--: None

#

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is Match or Do not match, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than Match and Do not match is selected, a business group name specified in a path format is treated as a host name.

If the -ignorecasehost option of the jcoimdef command is set to ON, and a comparison keyword other than Regular expression is selected, the character string is no longer case sensitive.

usr *user-name*

Specifies the user name of the JP1 user who executes the action. The usr parameter is optional. If this parameter is omitted, the system assumes the JP1 user name specified as the default action execution user in the definition of the automated action execution environment. If the default action execution user is also omitted, jp1admin is assumed.

The number of characters you can specify is 1 to 31 bytes for the user name. Only one-byte alphanumeric characters can be used. Alphabetic characters are not case sensitive. You can specify a variable for the user name. You specify a variable when you want to set information contained in the received JP1 event as the user name.

You can set event information for the user name.

When the action is executed, the JP1 user specified here is mapped to the OS user at the execution host that will execute the command, according to the JP1/Base definition. In UNIX, the shell environment of the mapped OS user is used for execution.

`hst` {*execution-host-name* | *group-name* | *business-group-name* | *monitoring-group-name*}

Specifies the name of the host on which an action is executed, a host group name, a business group name, or a monitoring group name. For a host name, specify a name set as a managed host in the system configuration definition. The `hst` parameter is optional. If it is omitted, the local host is assumed.

Express the execution host name or host group name using from 1 to 255 bytes of characters. The execution host name or host group name cannot contain the space character. You can specify a variable for the execution host name or host group name. You specify a variable when you want to set information contained in the received JP1 event as the execution host name or host group name. For example, to execute the action on the host that issues the event, specify `$EVHOST`.

You can set event information for the execution host name or host group name.

For a business group name and monitoring group name, you can specify a character string with a maximum of 2,048 bytes. If the specified character string begins with a slash (`/`), it is treated as a business group name or a monitoring group name. Note, however, that the character string is treated as a host name or a host group name if the integrated monitoring database and the IM Configuration Management database are disabled.

`cmd` *action*

Specifies the command that is to be executed as the action. For details about the specifiable commands, see *Chapter 6. Command Execution by Automated Action (JP1/Base linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The `cmd` parameter is optional. If this parameter is omitted, no action is taken even when conditions for action execution are satisfied.

Note that if any of the following parameters is omitted, omitting the `cmd` parameter results in a definition error:

`usr`, `var`, `hst`, `det`, `ret`

The `cmd` parameter cannot be specified more than once. Specify the parameter using from 1 to 4,096 bytes of characters. Any tabs or spaces preceding the action are deleted, but spaces following the action are not deleted.

You can set event information for the action.

You can use a variable to specify information contained in the received JP1 event. For example, if the execution host is UNIX, the following specification sets the name of the host that issued the JP1 event in the `HOSTNAME` environment variable:

`HOSTNAME="$EVHOST"` *action*

xxx`_BASIC="$EVBASE" xxx_MESSAGE="$EVMSG"` *action*

Notes about the length of an action command

The maximum length of a command that can be executed as an action is 4,096 bytes including the information obtained after converting variables to be used in the action definition (such as `$EVMSG`). If the command length exceeds 4,096 bytes, the execution status becomes `Fail`, in which case the command is not executed. In such a case, the message `KAVB4421-W` is displayed in the **Message** field in the Action Log Details window.

The length of a command that can be executed as an action also depends on the system where JP1/IM - Manager and JP1/Base are running.

If any of the hosts on the automated action execution route (including the source manager host and target execution host) runs JP1/IM - Manager or JP1/Base version 6 or version 7, the maximum length of a command must not exceed 1,024 bytes. For notes about the length of a command, see *13.4.1 Notes regarding the considerations for automated actions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Notes about codes that cannot be recognized as characters in an action

If codes (ASCII codes and characters not included in the character set of the multi-byte characters encoding specified in the environment settings) that are not recognizable as characters are included in an action, the action might not be executed, or if it is executed, might result in an error because of the shell or other specifications on the execution host. In such a case, the action results in terminated status, not an execution failure. Even though there might be no invalid code in the definition file, an invalid code might be generated when a variable used in the action definition is replaced with the actual value. For details about the correct specification of variables in an action definition, consult the documentation for the products that issue action-related events.

`var` *environment-variable-file-name*

Specifies the full path name of the environment variable file that specifies environment variables for the command that is to be executed as the action. This parameter is optional. If this parameter is omitted, it is assumed that there is no environment variable file. For details about the format of an environment variable file, see the *JP1/Base User's Guide*.

Express the environment variable file name using from 1 to 255 bytes of characters. You can set event information for the environment variable file name. You can specify a variable for the environment variable file name. You specify a variable when you want to set information contained in the received JP1 event as the environment variable file name. For example, to set the JP1 event extended attribute named `ENVFILE` as the environment variable file name, specify `$EV"ENVFILE"`.

Spaces before and after the environment variable file name are not deleted. Only one tab or one space character following `var` is deleted.

`det` *suppress-period*

Specifies a period during which action execution is to be suppressed. The action for the action conditions is suppressed if it would otherwise occur during the period specified in this parameter. This parameter is optional. If this parameter is omitted, the action is not suppressed. The permitted value range for the suppression period is from 1 to 3,600 (seconds). This parameter cannot be specified when you have specified `&` for the parameter group. In the case of AND conditions, specify the suppression period in the first automated action definition parameter that is defined for the AND conditions.

`ret` *delay-monitoring-period*

Specifies a period during which monitoring for the action execution is performed. If the amount of time specified in this parameter expires before a command control action termination message is received from the execution host after a JP1 event arrived at JP1/Base at the manager, a delay of action is reported by using a method such as JP1 event issuance or command execution. This parameter is optional. If this parameter is omitted, no monitoring for action delay is performed. The permitted value range for the delay monitoring period is from 1 to 86,400 (seconds).

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment. Note that if you set an action definition from JP1/IM - View, comment lines with the `#` mark are deleted.

Variables that can be used in the action definition

In a definition of automated action definition parameters, you can use variables in the `usr`, `var`, `hst`, and `cmd` parameters to specify information contained in the JP1 events.

When the action is executed, the variables are replaced with the actual information in the JP1 event.

To specify a variable in an automated action definition parameter, use a format such as `$EVID`. If you want to specify `$` as a character, specify the escape character `\` before the `$`.

The following table lists and describes the available variables.

Table 2–15: Variables that can be used in action definitions

Type of information	Variable name	Description
Information contained in the basic attributes of JP1 events	`EVBASE`	Entire basic event information[#1]
	`EVID`	Event ID (*basic-code*:*extended-code*)
	`EVIDBASE`	Event ID (basic code)

Type of information	Variable name	Description
	`EVDATE`	Event registration date (*YYYY*/*MM*/*DD*)#2
	`EVTIME`	Event registration time (*hh*:*mm*:*ss*)#2
	`EVPID`	Event source process ID
	`EVUSRID`	User ID of the event source process
	`EVGRPID`	Group ID of the event source process
	`EVUSR`	Event source user name
	`EVGRP`	Event source group name
	`EVHOST`	Event source host name
	`EVIPADDR`	Event source IP address
	`EVSEQNO`	Serial number
	`EVARVDATE`	Event arrival date (*YYYY*/*MM*/*DD*)#2
	`EVARVTIME`	Event arrival time (*hh*:*mm*:*ss*)#2
	`EVSRCNO`	Serial number at the event source
	`EVMSG`	Entire message text#3
	`EVDETAIL`	Entire detailed event information#3, #4
Information contained in the extended attributes of JP1 events	`EVSEV`	Severities in extended event information (`Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, `Debug`)#3
	`EVUSNAM`	User name#3
	`EVOBTYP`	Object type#3
	`EVOBNAM`	Object name#3
	`EVROBTYP`	Registration type#3
	`EVROBNAM`	Root object name#3
	`EV"PRODUCT_NAME"`	Product name#5
	`EV"OBJECT_ID"`	Object ID#5
	`EV"OCCURRENCE"`	Occurrence#5
	`EV"START_TIME"`	Start time#5
	`EV"END_TIME"`	End time#5
	`EV"RESULT_CODE"`	Return code#5
	`EV"JP1_SOURCEHOST"`	Issuing host name#5
	`EV"`*extended-attribute-name*`"`	Any extended attribute#5
Other	`EV"@JP1IM_CORRELATE"`	Correlation event flag • Not a correlation event: 0

Type of information	Variable name	Description
		• Correlation approval event: 1 • Correlation failure event: 2
	`EV"@JP1IM_ORIGINAL_SEVERITY"`	Extended event information original severity level (Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug)#3
	`EV"@JP1IM_CHANGE_SEVERITY"`	New severity level flag • Severity is not changed: 0 • Severity is changed: 1
	`EV"@JP1IM_DISPLAY_MESSAGE"`	Changed display message
	`EV"@JP1IM_CHANGE_MESSAGE"`	Display message change flag • Message has not been changed: `0` • Message was changed: `1`
	`ACTHOST`	Manager host name at the action request source#3
	`EVENV1` to `EVENV9`	Data obtained by specifying parentheses (`()`) in a regular expression in the specification of an action execution condition #5(applicable only when an extended regular expression is used at the manager host)

#1: The basic information of a JP1 event is converted to the following format and passed to the action (Δ indicates a single-byte space):

event-IDΔevent-source-user-nameΔevent-source-user-IDΔevent-source-group-nameΔevent-source-group-IDΔevent-source-event-server-nameΔevent-source-process-IDΔevent-registration-dateΔevent-registration-timeΔevent-source-host-IP-address

An item that is not set is replaced with the null character.

#2: Converted in the time zone for JP1/IM - Manager and passed to the action.

#3: When an action is executed, if the applicable attribute does not exist, the variable is converted to a null character and passed to the action.

#4: When detailed attribute information for a JP1 event is in binary format, the variable is converted to a null character and passed to the action.

#5: If the applicable attribute does not exist, the character string of the variable is passed to the action as is.

In addition, depending on the type of JP1 event, an action might not be executed, or if executed, might result in an error because the variable itself does not exist or codes (ASCII codes and characters that are not included in the character set of the multi-byte characters encoding specified in the environment settings) not recognizable as characters are included. See the documentation for the JP1 event source product to check the attribute information, and then set the characters that need to be replaced.

Encoding for event inheritance information

For **Action** of the action-related items, you can use URL encoding or Base64 encoding for the values for event inheritance information. The specification format is `$`*variable-name*`$`*encoding-type*. To specify a single-byte alphanumeric character or an underscore (_) immediately after *encoding-type*, use the format `${`*variable-name*`$`*encoding-type*`}`. If you specify a dollar sign (`$`) as part of a character string, immediate before `$`, specify `\` as an escape character.

In the following cases, `$`*variable-name*`$`*encoding-type* and `${`*variable-name*`$`*encoding-type*`}` will be treated as character strings and thus will not be converted:

- There is no event that corresponds to *variable-name*.
- The specification format is invalid.

The following table describes the encoding types for event inheritance information and shows the specification formats.

Table 2–16: Encoding types for event inheritance information and specification formats

No.	Encoding type	Specification format	Description
1	URL encoding	`$`*variable-name*`$URLENC`	URL encoding is used to encode the value of event inheritance information as a UTF-8 character string.
		`${`*variable-name*`$URLENC}`	
2	Base64 encoding	`$`*variable-name*`$ENC`	Base64 encoding is used to encode the value of event inheritance information.
		`${`*variable-name*`$ENC}`	
3	Both Base64 encoding and URL encoding	`$`*variable-name*`$ENC$URLENC`	The value of event inheritance information is encoded by using Base64 encoding and then by using URL encoding.
		`${`*variable-name*`$ENC$URLENC}`	
4	No encoding is performed	`$`*variable-name*	Neither URL encoding nor Base64 encoding is performed.
		`${`*variable-name*`}`	

Notes about specifying variables

- If you specify a character, such as an alphanumeric character or an underscore (_), immediately after the variable name, the variable will not be converted correctly. In such a case, enclose the variable name in curly brackets (`{ }`), as shown in the examples below. These examples assume that `100:0` is specified as the event ID (`$EVID`) and `ABC` is specified as the extended attribute `EX` (`$EV"EX"`).

  Examples:

  action-definition → *information-after-conversion*

  `$EVID abc` → `100:0 abc`

  `$EVIDabc` → `$EVIDabc` *(in Windows),* `none` *(in UNIX)*

  `${EVID}abc` → `100:0abc`

  `$EVID_abc` → `$EVID_abc` *(in Windows),* `none` *(in UNIX)*

  `${EVID}_abc` → `100:0_abc`

  `$EV"EX" abc` → `ABC abc`

  `$EV"EX"abc` → `ABCabc`

- If the source character information contains any of the control characters shown below, the control character is converted to a space (`0x20`).

  Control characters that are converted to a space: `0x01` to `0x1F` (excluding tab (`0x09`)), `0x7F`

  For example, if the message acquired by specifying `$EVMSG` contains a linefeed code (`0x0A`), the linefeed code (`0x0A`) is converted to the space (`0x20`).

  Example: If the action `echo $EVMSG` is set and the character string `"`*line-1* `0x0A` *line-2*`"`, which contains a linefeed code, is received as the message for the event, the command `"echo` *line-1Δline-2*`"` is executed as the action. (Δ indicates a single-byte space.)

- When a backslash (`\`) is specified immediately before a dollar sign (`$`), the dollar sign is treated as a character string. However, if you attempt to specify a backslash followed by a variable, for example, in a file path, the backslash will be converted instead of being treated as a character string. You can prevent this by one of the following methods:
  - Using an execution command:

    Create a batch file in which the variable is specified for the argument. Use the batch file to specify commands that include backslashes.

    Example of how to specify an execution command:

    • Execution command: `AppTest.bat $ACTHOST`

    • Batch file: `application.exe c:\work\%1\result.txt`

In this example, the conversion result of `$ACTHOST` is set for `%1`.

- Using a variable in a file path:

  Add a prefix to the variable.

  The following are examples of when `IM-VIEW` is set for `EV"PRODUCT_NAME"`.

  Example when the variable cannot be converted:

  • Example specification: `C:\$EV"PRODUCT_NAME"`

  • Conversion result: `C:$EV"PRODUCT_NAME"`

  In this example, `EV"PRODUCT_NAME"` cannot be converted because `\$` is specified.

  Example when the variable can be converted:

  • Example specification: `C:\pre_$EV"PRODUCT_NAME"`

  • Conversion result: `C:\pre_IM-VIEW`

  In this example, `EV"PRODUCT_NAME"` can be converted because `pre_` is added before the variable.

- In UNIX, the final expansion depends on the interpretation by the shell. If the expanded data contains a character that has a special meaning in the shell, such as `*`, it is replaced by the corresponding data. To prevent such characters from being converted, enclose the entire variable in double-quotation marks (`"`), such as `"$EVMSG"`.
- If JP1 event information specified by a variable contains a double quotation (`"`), single-quotation mark (`'`), or another character that has a special meaning when used in a command, the command might not be interpreted correctly. We recommend that you convert such characters in the configuration file for converting information. For details about the configuration file for converting information, see *Configuration file for converting information (event_info_replace.conf)* in *Chapter 2. Definition Files*.

Regular expressions in an action definition

This subsection describes how to use regular expressions to specify attributes of JP1 events (message text, basic attributes, and detailed information) in an event monitoring condition of an automated action definition.

The supported regular expressions depend on the OS. The regular expressions supported by Windows and UNIX are described below.

If you share the same action definitions among different OSs, specify conditions using expressions that are supported by all the OSs because interpretation of regular expressions depends on the OS. Regular expressions supported by all OSs are presented in *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. Consult this information to determine the regular expressions that can be used.

Regular expressions for the Windows version

For the Windows version, you can set the supported regular expressions to either JP1-specific regular expressions or extended regular expressions. The default is extended regular expressions. For details about how to specify JP1-specific regular expressions, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files*.

Regular expressions for the UNIX version

For the UNIX version, use the extended regular expressions. For details about the supported regular expressions, see the OS-provided *regexp(5)*.

Notes on regular expressions

- Because the regular expression of the automated action is a partial match, conditions are the same regardless of whether the same characters (`.*`) are specified for the first and last characters.

  For example, the same conditions can be set for the following examples 1 and 2:

Example 1: Regular expression matching the string containing "`A001Δ:ΔWEB-server`":

`.*A001Δ:ΔWEB-server.*`

Example 2: Regular expression matching the string containing "`A001Δ:ΔWEB-server`":

`A001Δ:ΔWEB-server`

Do not specify (`.*`) at the beginning or end because searching might take a long time.

- If the `jcamakea` command is executed to check a file that contains either of the regular expressions below, the `KAVB5759-W` message appears:
  - Regular expression beginning or ending with `.*`
  - Regular expression containing successive instances of `.*`

  For details about the `KAVB5759-W` message, see the *JP1/Integrated Management 3 - Manager Messages*.

Example definition

The examples below show example definitions for the automated action definition file. Note that the extended regular expression is specified as the regular expression type in these examples.

Example definition 1: Using a variable (1)

The following is an example definition for specifying JP1 event information received by using a variable as an argument of a command to be executed as an action:

- Event condition
  The event ID (`B.ID`) is `00000001`.

  The message format is *message-ID*#Δ:Δ*message-text*.

  #: A message ID consists of one alphabetic character and three numeric characters.
- Command to be executed as an action
  `alarm.bat`Δ*argument-1*Δ*argument-2*
- JP1 event information to be specified as a command argument
  argument-1: The message value (`${EVMSG}` is specified as a variable)
  argument-2: The extended attribute value `AAA` (`${EV"AAA"}` is specified as a variable)

```
 1 DESC_VERSION=3

 2 cmn
 3   sta△false
 4 end-cmn

 5 act△action 1
 6   prm△0
 7   cmt△Example of using a variable
 8   eid△1

 9   cnd
10     B.MESSAGE△REGEX△(^[A-Z][0-9][0-9][0-9])%20:%20(.*)
11   end-cnd

12   cmd△alarm.bat△"$EV"AAA""△"${EVMSG}"
13 end-act
```

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

When the value for the received JP1 event message (`B.MESSAGE`) is `A001Δ:ΔThe WEB server goes down.` and the value for the AAA extended attribute is `kanshi`, the action `alarm.batΔ"kanshi"Δ"A001Δ:ΔThe WEB server goes down."` is performed.

Example definition 2: Using a variable (2)

The following is an example definition for specifying a part of the JP1 event information received by using the variables `EVENV1` to `EVENV9` as arguments of the command to be executed as an action:

- Event condition

  The event ID (`B.ID`) is `00000001`.

  The message format is *message-ID*#Δ:Δ*message-text*.

  #: A message ID consists of one alphabetic character and three numeric characters.

- Command to be executed as an action

  `alarm.bat`Δ*argument-1*Δ*argument-2*

- JP1 event information to be specified as command arguments

  argument-1: Message ID value (`${EVENV1}` is specified as a variable)

  argument-2: Message text value (`${EVENV2}` is specified as a variable)

```
 1 DESC_VERSION=3

 2 cmn
 3   sta△false
 4 end-cmn

 5 act△action 1
 6   prm△0
 7   cmt△Example of using a variable
 8   eid△1

 9   cnd
10     B.MESSAGE△REGEX△(^[A-Z][0-9][0-9][0-9])%20:%20(.*)
11   end-cnd

12   cmd△alarm.bat△"${EVENV1}"△"${EVENV2}"
13 end-act

Note: In this example, a line number is inserted at the beginning of each line to indicate the
individual lines you need to write in the definition file.
```

When the value for the received JP1 event message (`B.MESSAGE`) is `A001Δ:ΔThe WEB server goes down.`, the action `alarm.batΔ"A001"Δ"The WEB server goes down."` is performed.

Example definition 3: Specifying an event ID in a regular expression (1)

The following is an example definition when `B.ID` is specified as the attribute name of an event condition and `REGEX` is specified as the comparison keyword:

- Event condition

  The event ID is a value from `00000001` to `00000200` (Hexadecimal A to F not included).

  The event-issuing server name (`B.SOURCESERVER`) is `kanshi`.

- Command to be executed as an action

  `alarm.bat`

```
 1 DESC_VERSION=3

 2 cmn
 3   sta△false
 4 end-cmn

 5 act△action 1
 6   prm△0
 7   cmt△Event ID:00000001 to 00000200
 8   eid△*

 9   cnd
10     B.ID△REGEX△(^0000000[1-9]|^000000[1-9][0-9]|^000001[0-9][0-9]|^00000200)
11     B.SOURCESERVER△IN△kanshi
12   end-cnd

13   cmd△alarm.bat
14 end-act
Note: In this example, a line number is inserted at the beginning of each line to
indicate the individual lines you need to write in the definition file.
```

To specify an event ID as an event condition, specify `*` for `eid` so that the event ID specified as an event condition becomes the target.

Example definition 4: Specifying an event ID in a regular expression (2)

If `B.BASIC` is specified for the attribute name as an event condition, the conditions can be set in the same format used for the basic event information of the automatic action definition file (for compatibility).

The following is an example definition when `B.BASIC` is specified as the attribute name of an event condition and `REGEX` is specified as the comparison keyword:

- Event condition

  The event ID is a value from `00000001` to `00000200` (Hexadecimal A to F not included).

  The event-issuing server name (`B.SOURCESERVER`) is `kanshi`.

- Command to be executed as an action

  `alarm.bat`

```
 1 DESC_VERSION=3

 2 cmn
 3   sta△false
 4 end-cmn

 5 act△action1
 6   prm△0
 7   cmt△Event ID:00000001 to 00000200
 8   eid△*

 9  cnd
10    B.BASIC△REGEX△(^[1-9]|^[1-9][0-9]|^1[0-9][0-9]|^200)
      :0%20.*%20.*%20.*%20.*%20kanshi%20.*%20.*%20.*%20.*$
11  end-cnd

12   cmd△alarm.bat
13 end-act

Note: In this example, a line number is inserted at the beginning of each line to indicate the
individual lines you need to write in the definition file.Line10 spans two lines here, but
write it as one line in the definition file.
```

The method for specifying a tab, space, %, or linefeed is different from the method used for the automatic action definition file (for compatibility). For details, see *Automated action definition file (actdef.conf) (for conversion)* in *Chapter 2. Definition Files*.

Example definition 5: Using the AND condition

The following is an example definition for setting the action to be executed when event A and event B are received:

- Event A conditions

  The event ID (`B.ID`) is `00000201`.

  The message (`B.MESSAGE`) is `WEB server A goes down.`.
- Event B conditions

  The event ID (`B.ID`) is `00000202`.

  The message (`B.MESSAGE`) is `Web server B goes down.`.
- Command to be executed as an action

  `alarm.bat`

```
 1 DESC_VERSION=3

 2 cmn
 3   sta△false
 4 end-cmn

 5 act△action 1
 6   prm△0
 7   cmt△Example of using AND condition (Event A conditions)
 8   eid△201

 9   cnd
10     B.MESSAGE△IN△WEB server A goes down.
11   end-cnd

12   cmd△alarm.bat
13 end-act

14 act
15   prm△&
16   cmt△Example of using AND condition (Event B conditions)
17   eid△202

18   cnd
19     B.MESSAGE△IN△WEB server B goes down.
20   end-cnd

21 end-act
```

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

When the AND condition is applied, we recommend using an automated action by using the correlation event generation function. The correlation event generation function can specify the sequence or the number of JP1 events, a property not available to the AND condition. For details about correlation events, see *4.3 Issue of correlation events* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Automated action definition file (actdef.conf) (for conversion)

Format

```
[#automated-action-definition-file-version]
[DESC_VERSION=version-information]

[#automated-action-status-monitoring-parameter]
Δ0[:state_watch={true | false}]

[#automated-action-definition-parameter]
Δ0[ {+parameter-group-number|&}Δ1] {$event-ID|*}Δ1
[/message/] [,[/basic-event-information/] [,[/detailed-event-information/]
[,[/event-levels-of-extended-event-information/] ] ] ]Δ1[attribute-name-of-ex
tended-event-information=/attribute-value/
[,attribute-name-of-extended-event-information2=/attribute-value/][,...] ]Δ0
: Δ0[u=user-nameΔ1] [e=environment-variable-file-nameΔ1]
[d=execution-host-name|group-nameΔ1] [dt=suppress-periodΔ1]
[rt=delay-monitoring-periodΔ1] [action]
   :
```

File

`actdef.conf` (automated action definition file) (for conversion)

Storage directory

In Windows

For a physical host:

Console-path`\conf\action\`

For a logical host:

shared-folder`\jp1cons\conf\action\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/action/`

For a logical host:

shared-directory`/jp1cons/conf/action/`

Description

This file defines (for conversion) conditions for executing actions by the automated action function of JP1/IM and the commands to be executed as the actions. Use the language encoding that is used by JP1/IM - Manager to specify this file.

When a JP1 event satisfying specified conditions is received, the automated action function executes automatically a specified command based on the definition specified in this file.

Each line of action definition information is called a *parameter*. There are three types of parameters in an automated action definition file:

- Automated action definition file version

Defines the format version of the automated action definition file.

- Automated action status monitoring parameter

  Defines whether the status of automated actions is to be monitored.

- Automated action definition parameters

  Define conditions for executing an action and the command to be executed as the action.

You must specify the automated action definition file version and the automated action status monitoring parameter before the automated action definition parameters. If you specify the automated action definition file version and/or the automated action status monitoring parameter after any automated action definition parameters, the specified definition is ignored.

If you specify the automated action definition file version or the automated action status monitoring parameter more than once, the first definition specified takes effect and subsequent definitions are ignored.

Definition specification

The automated action status monitoring parameter and the automated action definition parameters specify one definition per line. A definition that will not fit on one line can be continued onto the next line.

An automated action definition parameter is specified in the format *event-monitoring-condition*`:`*action-execution-definition*, consisting of two components separated by a colon (`:`).

- The maximum length of one automated action definition parameter is 5,706 bytes.

  Spaces are counted, but the `\` in a linefeed code or in a continuation line indicator is not counted.

- An automated action definition parameter that will not fit on one line can continue onto the next line.

  To continue a definition onto the next line, specify `\` immediately before the linefeed code at the end of the line. If there is any character, including a space, between `\` and the linefeed code, the `\` will be regarded as data.

- A line containing a hash mark (`#`) in column 1 is regarded as a comment line.

  A comment must be specified on a single line. If a comment consists of multiple lines, all but the first line will be discarded when the GUI is used for specifying the definition. Any hash marks (`#`) in columns other than column 1 or on continuation lines are treated as data, not as a comment.

Priority order of event monitoring conditions

If a received JP1 event satisfies the execution conditions in multiple automated action definitions, only the automated action that has the highest priority level is executed (for each parameter group discussed below). The automated action priority order is determined by the following rules:

- For automated actions with an event ID specified, an automated action that is applied to all event IDs takes precedence.
- The first action specified in the automated action definition file (in GUI, the first action displayed in the Action Parameter Definitions) takes precedence.

Parameter groups and AND conditions

Each automated action definition parameter belongs to a parameter group. A parameter group is a unit for checking the conditions for executing an automated action. Use of parameter groups allows you to specify complex conditions, such as when multiple actions are to be executed for a single JP1 event or when an action is to be executed only when multiple conditions are satisfied.

When a single JP1 event arrives at the manager of JP1/IM, the automated action definition parameters and execution conditions are compared for each parameter group in order of priority. When execution conditions that are satisfied are found, only the automated action definition parameter that has the highest priority is executed for each parameter group.

If you specify an ampersand (`&`) in a parameter group, an AND condition with the automated action definition parameter defined on the preceding line is created. When automated action definition parameters are specified in an AND condition, the corresponding action is executed when all the conditions are satisfied.

Checking the size of an automated action definition parameter

The following lists the items whose size is checked and the respective maximum sizes:

- The maximum size of an automated action definition parameter is 5,706 bytes.
- In an automated action definition parameter, the maximum size of the event monitoring conditions is 1,040 bytes.
- In an automated action definition parameter, the maximum size of an action is 4,096 bytes.

If a maximum size is exceeded, a message is displayed when the definition is applied and the corresponding automated action definition parameter is ignored.

Checking the specified information

Use the `jcamakea` command to check the information specified in the definition file.

Note that, for the automated action definition file (`actdef.conf`) (for compatibility), a business group name cannot be used. If a business group name is specified, it is treated as a host name.

When the definitions are applied

The definition of an automated action takes effect when you click the **Apply** button in the Action Parameter Definitions window in JP1/IM - View when JP1/IM - Manager starts, or when you execute the `jcachange` command.

If you want to execute the `jcachange` command to re-load the definition, execute the `jcamakea` command first to make sure there are no errors in the definition.

Information that is specified (automated action definition file version)

This subsection describes the information to be specified as the automated action definition file version.

`DESC_VERSION=`*version-information*

Defines the format version of the automated action definition file.

Table 2–17: Automated action definition file format version information

Version information	Description
1	Automated action definition file version is 07-11 to 07-51.
2	Automated action definition file version is 08-01 or later.
3	Automated action definition file version is 09-00 or later.
4	Automated action definition file version is 11-50 or later.

If this parameter is omitted or `1` is specified, the value `2` is assumed for reading the file. When the **Apply** button is clicked in the Action Parameter Definitions window in JP1/IM - View, the value `2` is set.

If a value other than `1`, `2`, `3`, or `4` is specified in this parameter, an error is output to the integrated trace log, and the value `3` is assumed as the version information for reading the file. In such cases, the Action Parameter Definitions window cannot be displayed in JP1/IM - View. To change the version information, edit the definition file.

Because the format of an old automated action definition file version is compatible with the automated action definition file format for version 08-01 or later, the format for version 08-01 or later is assumed for reading the file.

If this parameter is specified on a line that is subsequent to a line containing an automated action definition parameter, the Action Parameter Definitions window can no longer be displayed in JP1/IM - View.

Use the `jcamakea` command to check the contents of the automated action definition file.

Information that is specified (automated action status monitoring parameter)

This subsection describes the information to be specified in the automated action status monitoring parameter.

`state_watch={true | false}`

Specifies whether the action status is to be monitored.

Specify either `true` or `false`. The default is `false`.

If `true` is specified, the Action Parameter Definitions window cannot be displayed in JP1/IM - View version 07-01 or earlier.

This parameter is effective only if it is specified before the automated action definition parameters.

If this parameter is specified on a line that is subsequent to a line containing an automated action definition parameter, the Action Parameter Definitions window can no longer be displayed in JP1/IM - View.

You should use the `jcamakea` command to check the contents of the automated action definition file.

When JP1/IM - View version 07-11 or later is connected to JP1/IM - Manager (Central Console) version 07-11 or later, the automated action status monitoring parameter will always be output to the automated action definition file even when the action status is not being monitored.

Information that is specified (automated action definition parameters)

This subsection describes each item that is specified in the automated action definition parameters. For details about the JP1 events, see *Chapter 3. JP1 Events*. Regular expressions and variables that can be specified in the definition are described later.

Event monitoring conditions

The items to be specified as the execution conditions in an automated action definition parameter are described below. The maximum length of a parameter that can be defined as execution conditions is 1,040 bytes.

`{`+*parameter-group-number*`|&}`

Specifies the parameter group number to which the automated action definition parameter on this line belongs, expressed as a single-digit number (from 0 to 9) preceded by a plus sign (+). If this information is omitted, `0` is assumed.

If you specify an ampersand (`&`), this parameter becomes part of an AND condition with the immediately preceding definition line, which means that the automated action definition parameter on this line belongs to the same parameter group as the parameter on the immediately preceding line.

Note that the parameter group number has nothing to do with the priority order for checking execution conditions or the sequence of executing actions.

`$`*event-ID*

Specifies the event ID preceded by the dollar sign (`$`). The specification format of an event ID is as follows:

basic-part`[`:*extended-part*`]`

Specify the basic and extended parts each using from 1 to 8 hexadecimal numbers (from `0` to `7FFFFFFF`). Alphabetic characters must be specified as lowercase letters.

`*`

Specifies that the target is all event IDs. When an asterisk (`*`) is specified, all events become subject to the action. If JP1 events occur frequently, a large number of actions will be implemented, in which case execution may be delayed. When you specify an asterisk, you should narrow down the applicable events by using other conditions (such as a message, basic event information, detailed event information, and extended event information).

message

Specifies as an execution condition a message text associated with the JP1 event. You can use a regular expression for the condition. When you use a regular expression, specify the message text without control codes.

To express `/` in a regular expression, specify `\/`.

basic-event-information

Specifies information about JP1 event basic attributes that are to be used as an execution condition. You can use a regular expression to specify this information.

To express `/` in a regular expression, specify `\/`. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The basic event information is passed as information about JP1 event basic attributes in the format shown below. Use this format to specify a condition for executing an action.

*event-ID*Δ*event-source-user-name*Δ*event-source-user-ID*Δ

*event-source-group-name*Δ*event-source-group-ID*Δ

*event-issuing-server-name*Δ*event-source-process-ID*Δ

*event-registration-year-month-day*Δ*event-registration-time*Δ*event-source-host-IP-address*

For details about the information included in the JP1 event basic attributes, see *Chapter 3. JP1 Events*.

detailed-event-information

Specifies information about detailed attributes in the JP1 event basic attributes that is to be used as an execution condition.

You can use a regular expression to specify this information.

To express `/` in a regular expression, specify `\/`. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The detailed attributes in the JP1 event basic attributes consist of additional JP1 event information. The details and format of this information depend on the JP1 event. If the detailed attribute information is specified in binary format, it is treated as no information (NULL).

Remarks: The detailed attributes in the JP1 event basic attributes are used principally to record detailed information provided by products that issue events that are compatible with the JP1/SES format of version 5 or earlier. Most products whose version is 6 or later use the JP1 event extended attributes to record detailed information.

event-levels-of-extended-event-information

Specifies the severity levels in the extended attributes of the JP1 events that are to be set as an execution condition. Specify the event levels (severities) by combining the applicable characters in the following format:

```
-------E Event level:Emergency
------A- Event level:Alert
-----C-- Event level:Critical
----E--- Event level:Error
---W---- Event level:Warning
--N----- Event level:Notice
-I------ Event level:Information
```

```
D------- Event level:Debug
```

For example, to set as a condition all severities at the Error and higher event levels, specify `/----ECAE/`.

attribute-name-of-extended-event-information=/*attribute-value*/

Specifies a combined name and value of the JP1 event extended attribute used to form an execution condition. You can use a regular expression to specify this information.

To express `/` in a regular expression, specify `\/`.

You can specify a maximum of 100 pairs of attribute name and attribute value combinations.

For an attribute name, you can specify from 1 to 32 bytes of uppercase letters, numeric characters, and the underscore (_). The attribute name cannot contain a colon (`:`) or an equal sign (=). Specify an attribute name in a form such as `PRODUCT_NAME` or `OBJECT_NAME`. Unlike the settings in other functions, this attribute name is not prefixed with `E.`.

If you specify an event level in this item (item name `SEVERITY`), specify the attribute value as a character string, such as `Emergency` or `Alert`.

Action execution definition

The following describes the items in an automated action definition parameter that can be used to specify an action execution definition.

`u=`*user-name*

Specifies the user name of the JP1 user who executes the action.

You can specify 1 to 31 bytes of characters. Only one-byte alphanumeric characters can be used. Alphabetic characters are not case sensitive.

If this parameter is omitted, the system assumes the JP1 user name specified as the default action execution user in the definition of the automated action execution environment. If the default action execution user is also omitted, `jp1admin` is assumed.

You can use a variable to specify information contained in the received JP1 event as the JP1 user name.

When the action is executed, the JP1 user specified here is mapped to the OS user at the execution host that will execute the command, according to the JP1/Base definition. In UNIX, the shell environment of the mapped OS user is used for execution.

`e=`*environment-variable-file-name*

Specifies the full path name of the environment variable file that specifies environment variables for the command that is to be executed as the action.

The file name can be a character string with a maximum size of 255 bytes. If the file name contains a space, enclose the entire name in double-quotation marks (`""`).

You can use a variable to specify information contained in the received JP1 event as the file name. For example, to set the JP1 event extended attribute named `ENVFILE` as the environment variable file name, specify `$EV"ENVFILE"`.

For details about the format of the environment variable file, see the *JP1/Base User's Guide*.

`d=`*execution-host-name*|*group-name*

Specifies the name of the host or host group that is to execute the action. For a host name, specify a name set as a managed host in the system configuration definition. A host name or host group name cannot contain a space.

If this parameter is omitted, the action is executed at the local host (the host that contains the automated action definition file).

You can use a variable to specify information contained in the received JP1 event as the host name or group name. For example, to execute the action on the host that issued the event, specify `$EVHOST`.

`dt=`*suppress-period*

Specifies a period during which action execution is to be suppressed. The action for the action conditions is suppressed if it would occur during the period specified in this parameter. If this parameter is omitted, the action is not suppressed. Express the suppression period using from 1 to 4 bytes of numeric characters. The permitted value range is from 1 to 3,600 (seconds).

When this parameter is specified, JP1/IM - View version 07-01 or earlier cannot display the Action Parameter Definitions window.

Note that this parameter cannot be specified in the following case:

`&` is specified.

`rt=`*delay-monitoring-period*

Specifies a period during which monitoring for the action execution is performed. If the amount of time specified in this parameter expires before a command control action termination message is received from the execution host after a JP1 event arrived at JP1/Base at the manager, a delay of action is reported by using a method such as JP1 event issuance or command execution. This parameter is optional. If this parameter is omitted, no monitoring for action delay is performed.

Express the delay monitoring period using a maximum of five bytes of numeric characters. The permitted value range for the delay monitoring period is from 1 to 86,400 (seconds).

When this parameter is specified, JP1/IM - View version 07-01 or earlier cannot display the Action Parameter Definitions window.

action

Specifies the command that is to be executed as the action.

For details about the specifiable commands, see *Chapter 6. Command Execution by Automated Action (JP1/Base linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If this parameter is omitted, no action is taken even when conditions for action execution are satisfied.

You can use a variable to specify information contained in the received JP1 event as the command parameter.

If the host where the automated action is defined is UNIX, you can use a variable to specify information contained in the received JP1 event as the command environment variable. For example, `MESSAGE="$EVMSG" command arg1 arg2` can be specified.

Note that the colon (`:`) in the automated action definition parameter is followed by the action to be executed. If you simply specify `u=`, `e=`, `d=`, `dt=`, or `rt=`, it is treated as being part of the previous information, such as a user name. If you specify information such as `u=` and omit the action, an error will result.

The maximum length of a command that can be executed as an action is 4,096 bytes, including the information obtained after converting variables to be used in the action definition (such as `$EVMSG`). If the command length exceeds 4,096 bytes, the execution status becomes `Fail`, in which case the command is not executed. In such a case, the message `KAVB4421-W` is displayed in the **Message** field in the Action Log Details window.

If codes (ASCII codes and characters not included in the character set of the multi-byte characters encoding specified in the environment settings) that are not recognizable as characters are included in an action, the action might not be executed or, if it is executed, might result in an error because of the shell or other specifications on the execution host. If an action contains a code that cannot be recognized as a character, the action might not be executed by the shell at the execution host or might result in an error when the action attempts to execute. In such a case, the action results in terminated status, not an execution failure. Even though there might be no invalid code in the definition file, an invalid code might be generated when a variable used in the action definition is replaced with the actual value. For details about the correct specification of variables in an action definition, consult the documentation for the products that issue action-related events.

Notes about the length of an action command

The maximum length of a command that can be executed as an action depends on the system where JP1/IM - Manager and JP1/Base are running.

If any of the hosts on the automated action execution route (including the source manager host and target execution host) runs JP1/IM - Manager or JP1/Base version 6 or version 7, the maximum length of a command must not exceed 1,024 bytes. For notes about the length of a command, see *13.4.1 Notes regarding the considerations for automated actions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Variables that can be used in the action definition

In a definition of automated action definition parameters, you can use variables in the specification of the action to be executed (specification following a colon (**:**)) to set information contained in the JP1 event. When the action is executed, the variables are replaced with the actual information in the JP1 event.

To specify a variable in an automated action definition parameter, use a format such as `$EVID`.

The following table lists the describes the available variables.

Table 2–18: Variables that can be used in the action definition

Type of information	Variable name	Description
Information contained in the basic attributes of JP1 events	`EVBASE`	Entire basic event information
	`EVID`	Event ID (*basic-code*:*extended-code*)
	`EVDATE`	Event generation date (*YYYY*/*MM*/*DD*)
	`EVTIME`	Event generation time (*hh*:*mm*:*ss*)
	`EVPID`	Event source process ID
	`EVUSRID`	User ID of the event source process
	`EVGRPID`	Group ID of the event source process
	`EVUSR`	Event source user name
	`EVGRP`	Event source group name
	`EVHOST`	Event source host name
	`EVIPADDR`	Event source IP address
	`EVSEQNO`	Serial number
	`EVARVDATE`	Event arrival date (*YYYY*/*MM*/*DD*)
	`EVARVTIME`	Event arrival time (*hh*:*mm*:*ss*)
	`EVSRCNO`	Serial number at the event source
	`EVMSG`	Entire message text
	`EVDETAIL`	Entire detailed event information
Information contained in the extended attributes of JP1 events	`EVSEV`	Severities in extended event information (`Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, `Debug`)
	`EV"`*extended-attribute-name*`"`	Any extended attribute
Other	`ACTHOST`	Manager host name at the action request source

Type of information	Variable name	Description
	`EVENV1` to `EVENV9`	Data obtained by specifying parentheses (`()`) in a regular expression in the specification of an action execution condition (applicable only when an extended regular expression is used at the manager host)

The value of the variable for an invalid item is NULL. In addition, depending on the type of JP1 event, an action might not be executed, or if executed, might result in an error because the variable itself does not exist or codes (ASCII codes and characters not included in the character set of the multi-byte characters encoding specified in the environment settings) that are not recognizable as characters are included. Consult the documentation for the products that issue JP1 events beforehand for correct specification of the information.

Notes about specifying variables

- If you specify a character, such as an alphanumeric character or an underscore (_), immediately after the variable name, the variable will not be converted correctly. In such a case, enclose the variable name in curly brackets (`{ }`), as shown in the examples below. These examples assume that `100:0` is specified as the event ID (`$EVID`) and `ABC` is specified as the extended attribute `EX` (`$EV"EX"`).

  Examples:

  action-definition → *information-after-conversion*

  `$EVID abc` → `100:0 abc`

  `$EVIDabc` → `$EVIDabc` *(in Windows),* `none` *(in UNIX)*

  `${EVID}abc` → `100:0abc`

  `$EVID_abc` → `$EVID_abc` *(in Windows),* `none` *(in UNIX)*

  `${EVID}_abc` → `100:0_abc`

  `$EV"EX" abc` → `ABC abc`

  `$EV"EX"abc` → `ABCabc`

- If the source character information contains any of the control characters shown below, the control character is converted to a space (`0x20`).

  Control characters that are converted to a space: `0x01` to `0x1F` (excluding tab (`0x09`)), `0x7F`

  For example, if the message acquired by specifying `$EVMSG` contains a linefeed code (`0x0A`), the linefeed code (`0x0A`) is converted to the space (`0x20`).

  Example: If the action `echo $EVMSG` is set and the character string "*line-1* `0x0A` *line-2*", which contains a linefeed code, is received as the message for the event, the command "`echo` *line-1*Δ*line-2*" is executed as the action (Δ indicates a space).

- In UNIX, the final expansion depends on the interpretation by the shell. If the expanded data contains a character that has a special meaning in the shell, such as `*`, it is replaced by the corresponding data. To prevent such characters from being converted, enclose the entire variable in double-quotation marks (`"`), such as `"EVMSG"`.

- If a JP1 event specified by using a variable contains a double quotation (`"`), single-quotation mark (`'`), or another character that has a special meaning when used in a command, the command might not be interrupted correctly. We recommend that you convert such characters in the configuration file for converting information. For details about configuration file for converting information, see *Configuration file for converting information (event_info_replace.conf)*in *Chapter 2. Definition Files*.

Regular expressions in the action definition

This subsection describes how to use regular expressions to specify the attributes of JP1 events (message text, basic attributes, and detailed information) in an event monitoring condition of an automated action definition.

The supported regular expressions depend on the OS. The regular expressions supported by Windows and UNIX are described below.

If you share the same action definitions among different OSs, specify conditions using expressions that are supported by all the OSs because interpretation of regular expressions depends on the OS. Regular expressions supported by all OSs are presented in *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. Consult this information to determine the regular expressions that can be used.

Regular expressions for the Windows version

For the Windows version, you can set the supported regular expressions to either JP1-specific regular expressions or extended regular expressions. The default is extended regular expressions. For details about how to use the JP1-specific regular expressions, see *Automated action environment definition file (action.conf.update)* in *Chapter 2. Definition Files*.

In the case of automated actions in JP1/IM, you can also use the extended notations shown below, in addition to the OS's regular expressions:

`\/`, `\\`

Even in an expression enclosed in brackets, / and \ are treated as characters. This method is used to specify / and \ in regular expressions.

Regular expressions for the UNIX version

For the UNIX version, use the extended regular expressions. For details about the supported regular expressions, see the OS-provided *regexp(5)*.

In the case of automated actions in JP1/IM, you can also use the extended notations shown below, in addition to the OS's regular expressions:

`\/`, `\\`

Even in an expression enclosed in brackets, / and \ are treated as characters. This method is used to specify / and \ in regular expressions.

Specifying the basic and detailed attributes using regular expressions

This subsection describes how to use regular expressions to specify basic attributes and detailed information about JP1 events in the event monitoring conditions.

The basic attributes of a JP1 event are expressed in the automated action definition parameters in the following format:

event-ID#1Δ*event-source-user-name*Δ*event-source-user-ID*Δ

*event-source-group-name*Δ*event-source-group-ID*Δ

event-issuing-server-name#2Δ*event-source-process-ID*Δ

event-registration-year-month-day#3Δ*event-registration-time*#4Δ*event-source-host-IP-address*

#1

The event ID is expressed in the format *basic-code*:*extended-code*. The basic code and extended code are each an 8-digit hexadecimal number (characters from `A` to `F` must be uppercase). Any leading zeros in the ID are omitted. If the extended code is `00000000`, the event ID is expressed as *basic-code*:`0`.

#2

In the event that the server name differs from the host name and the method for acquiring the event issuing host name is set to `local`, the host name is used, not the event server name.

#3

Expressed in the format *YYYY*/*MM*/*DD*.

#4

The event registration time is expressed in the format *hh*:*mm*:*ss*.

The detailed information about a JP1 event is expressed in the following format:

*information-1*Δ*information-2*Δ*information-3*Δ...Δ*information-n*Δ

Note:

Depending on the program, the detailed information might not be in this format or it might contain codes that cannot be recognized as characters, such as when only one byte of a multi-byte character is included because of fixed-length requirements. For details about the format, see the documentation for each program.

For both basic attributes and detailed information, each item in the information is separated by a space.

When there is no corresponding information, the item is treated as NULL and multiple consecutive delimiter spaces are displayed. Note that in the future more information might be added after the last item due to functionality extensions.

How to specify each item in the basic attributes and the detailed information is described below.

When you specify the first item in the basic attributes and detailed information, use a caret (`^`) to indicate the start of a character string. For example, the following specifies the JP1 event whose event ID is `00003A80`:

```
^3A80
```

In specifying the second and subsequent items, use `.*` (indicating any character string or space) to skip each unneeded item. For example, to specify the event issuing host name, which is the 6th item in the basic event attributes, repeat `.*` five times, as follows:

```
^.*Δ.*Δ.*Δ.*Δ.*Δhost01
```

The following are examples of specifying event information:

Example 1: JP1 event sent from the user whose user name begins with `JP1USER`:

```
^.*ΔJP1USER[_A-Z0-9]+Δ.*Δ.*Δ.*Δ.*Δ.*Δ.*Δ.*Δ.*$
```

Example 2: JP1 event issued at `host01` to `host05` (when an extended regular expression is used):

```
^.*Δ.*Δ.*Δ.*Δ.*Δhost0[1-5]Δ.*Δhost0[1-5]Δ.*Δhost0[1-5]Δ.*Δhost0[1-5]Δ.$
```

Example 3: JP1 event registered from 08:00 to 08:10 at `host02` (when a extended regular expression is used):

```
^.*Δ.*Δ.*Δ.*Δ.*Δhost02Δ.*Δ.*Δ08:(10|0[0-9]).*Δ.*$
```

Example 4: JP1 event whose third item begins with `prn` in the detailed information:

```
^.*Δ.*Δprn.*$
```

Note: For the format of detailed information, see the documentation of the program that issues the JP1 events.

Notes about regular expressions

- To use extended regular expressions by extending JP1-specific regular expressions (Windows), you must re-evaluate the existing definition settings and redefine them for extended regular expressions in order to avoid any malfunction that might be caused by the extension.

  The handling of control codes (such as linefeeds and tabs) might vary depending on the product and OS. If you use a regular expression to specify a message as a condition, specify only the message text without the control codes.

- Because the regular expression of the automated action is a partial match, conditions when the same characters (`.*`) are specified as the first and the last characters and when they are not specified are the same.

  For example, the same conditions can be set for the following examples 1 and 2:

  Example 1: Regular expression matching the string containing "`A001Δ:Δ`WEB-server":

  `.*A001Δ:Δ`*WEB-server*`.*`

  Example 2: Regular expression matching the string containing "A001Δ`:`ΔWEB-server":

  `A001Δ:Δ`*WEB-server*

  Do not specify (`.*`) at the beginning or end because searching might take a long time.

- The vertical bar `|`, which is a special character, represents the OR condition. When you use this OR condition in regular expressions, note the following:

  Because the vertical bar `|` indicating an OR condition has a low priority level, you must explicitly specify the range of the OR condition. Omitting the range might result in no operation or a malfunction. To specify the range of an OR condition, enclose it in parentheses `()`. The example below specifies an OR condition for the event-issuing server name.

  Example: JP1 event issued at `gyoumu` or `host`:

  `^.*Δ.*Δ.*Δ.*Δ.*Δ(gyoumu|host)Δ.*Δ.*Δ.*Δ.*$`

Example definition

The examples below show example definitions for the automated action definition file. Note that the extended regular expression is specified as the regular expression type in these examples.

Example definition 1: Using a variable (1)

The following is an example definition for specifying JP1 event information received by using a variable as an argument of a command to be executed as an action:

- Event condition

  The event ID (`B.ID`) is `00000001`.

  The message format is *message-ID*[#]Δ:Δ*message-text*.

  #: A message ID consists of one alphabetic character and three numeric characters.

- Command to be executed as an action

  `alarm.bat`Δ*argument-1*Δ*argument-2*

- JP1 event information to be specified as a command argument

  argument-1: The message value (`${EVMSG}` is specified as a variable)

  argument-2: The extended attribute `AAA` (`${EV"AAA"}` is specified as a variable)

```
1 DESC_VERSION=2
2 :state_watch=false
3 #Example of using a variable
4 +0△$1△/(^[A-Z][0-9][0-9][0-9])△:△(.*)/,,,△:alarm.bat△"$EV"AAA""△"${EVMSG}"
```

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

When the value for the received JP1 event message (`B.MESSAGE`) is `A001Δ:ΔThe WEB server goes down.`, and the value for the AAA extended attribute is `kanshi`, the action, `alarm.batΔ"kanshi"Δ"A001Δ:ΔThe WEB server goes down."` is performed.

Example definition 2: Using a variable (2)

The following is an example definition for specifying a part of the JP1 event information received by using the variables `EVENV1` to `EVENV9` as arguments of the command to be executed as an action:

- Event condition

  The event ID (`B.ID`) is `00000001`.

  The message format is *message-ID*[#]Δ:Δ*message-text*.

  #: A message ID consists of one alphabetic character and three numeric characters.

- Command to be executed as an action

  `alarm.bat`Δ*argument-1*Δ*argument-2*

- JP1 event information to be specified as a command argument

  argument-1: Message ID value (`${EVENV1}` is specified as a variable)

  argument-2: Message text value (`${EVENV2}` is specified as a variable)

```
1 DESC_VERSION=2
2 :state_watch=false
3 #Using a variable
4 +0△$1△/(^[A-Z][0-9][0-9][0-9])△:△(.*)/,,,△:alarm.bat△"${EVENV1}"△"${EVENV2}"

Note: In this example, a line number is inserted at the beginning of each line to indicate the
individual lines you need to write in the definition file.
```

When the value for the received JP1 event message (`B.MESSAGE`) is `A001Δ:ΔThe WEB server goes down.`, the action, `alarm.batΔ"A001"Δ"The WEB server goes down."` is performed.

Example definition 3: Specifying an event ID in a regular expression

The following is an example definition when `REGEX` is specified as the comparison keyword and `B.ID` is specified as the attribute name of an event condition:

- Event condition

  The event ID is a value from `00000001` to `00000200` (Hexadecimal A to F not included).

  The event-issuing server name (`B.SOURCESERVER`) is `kanshi`.

- Command to be executed as an action

  `alarm.bat`

```
1 DESC_VERSION=2
2 :state_watch=false
3 #The event ID is a value from 00000001 to 00000200 (Hexadecimal A to F not included).
4 +0△*△,/(^[1-9]|^[1-9][0-9]|^1[0-9]
  [0-9]|^200):0△.*△.*△.*△.*△kanshi△.*△.*△.*△.*$/,,△:alarm.bat

Note: In this example, a line number is inserted at the beginning of each line to indicate the
individual lines you need to write in the definition file.
Line 4 spans two lines here, but write it as one line in the definition file.
```

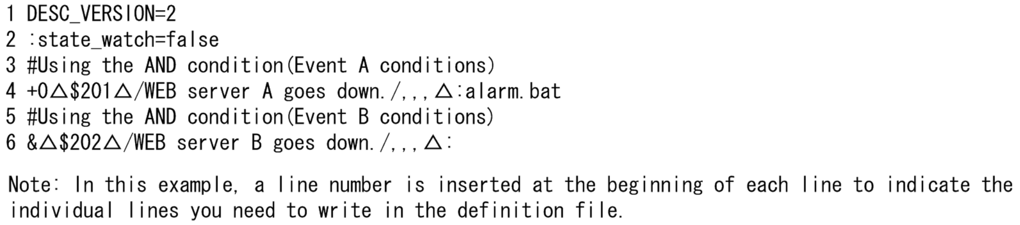
To specify an event ID in event basic information, specify `*` for `eid` so that the event ID specified in event basic information is to be the target.

In addition, specify a hexadecimal value with a maximum of eight bytes for the basic section and the extended section of an event ID and separate the sections by a colon (`:`).

Example definition 4: Using the AND condition

The following is an example definition for setting the action to be executed when event A and event B are received:

- Event A conditions
  The event ID (`B.ID`) is `00000201`.
  The message (`B.MESSAGE`) is `WEB server A goes down.`.
- Event B conditions
  The event ID (`B.ID`) is `00000202`.
  The message (`B.MESSAGE`) is `Web server B goes down.`.
- Command to be executed as an action
  `alarm.bat`



```
1 DESC_VERSION=2
2 :state_watch=false
3 #Using the AND condition(Event A conditions)
4 +0△$201△/WEB server A goes down./,,,△:alarm.bat
5 #Using the AND condition(Event B conditions)
6 &△$202△/WEB server B goes down./,,,△:
```

Note: In this example, a line number is inserted at the beginning of each line to indicate the individual lines you need to write in the definition file.

When the AND condition is applied, we recommend using an automated action by using the correlation event generation function. The correlation event generation function can specify the sequence or the number of JP1 events, a property not available to the AND condition. For details about the correlation events, see *4.3 Issue of correlation events* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Automatic action notification definition file (actnotice.conf)

Format

```
[STATE_WATCH]
EVENT={true | false}
COMMAND=command
[End]
[DELAY_WATCH]
EVENT={true | false}
COMMAND=command
[End]
```

File

`actnotice.conf` (automatic action notification definition file)

`actnotice.conf.model` (model file for the automatic action notification definition file)

Storage directory

In Windows

- For a physical host:
  - *Console-path*`\conf\action\`
- For a logical host:
  - *shared-folder*`\jp1cons\conf\action\`

In UNIX

- For a physical host:
  - `/etc/opt/jp1cons/conf/action/`
- For a logical host:
  - *shared-directory*`/jp1cons/conf/action/`

Description

This file defines whether a notification is to be issued when automated action status monitoring or delay monitoring detects an error in an automated action. The notification can be to issue a JP1 event or to execute a notification command. Specify this file by using the language encoding that is used by JP1/IM - Manager.

When you specify in this definition file that notification is to be performed in the event of an automated action error, you will be able to detect an automated action that terminates abnormally in `Fail`, `Error`, or `Fail (Miss)` status by monitoring the automated action status. In such a case, you can specify that a JP1 event is to be issued or that a notification command is to be executed to prompt the operator to take appropriate action for the erroneous automated action. The automated action delay monitoring function enables you to detect an automated action that does not terminate within a specified amount of time (the delay monitoring period) and to issue a JP1 event or execute a notification command to prompt the operator to take appropriate action for the automated action that is in delayed status.

If you have deleted the automatic action notification definition file (`actnotice.conf`), copy the model file for automatic action notification definition file (`actnotice.conf.model`) under the name `actnotice.conf` and change the definitions as necessary.

When the definitions are applied

The settings in the automatic action notification definition file take effect at the following times

- When JP1/IM - Manager starts
- When the file is reloaded by the `jco_spmd_reload` command

Information that is specified

`[STATE_WATCH]`

Defines whether to provide notification about an automated action error that is detected during automated action status monitoring by issuing a JP1 event or executing a notification command.

`EVENT={true | false}`

Specifies whether a JP1 event (event ID: `2011`) is to be issued when an error is detected during automated action status monitoring.

Specify either `true` or `false`. If you want to issue a JP1 event when an error is detected, specify `true`; otherwise, specify `false`. The default is `true`. When `true` is specified, a JP1 event (event ID: `2016` or `2021`) is also issued in the following cases:

Suppression of notification to the action status monitoring function is released (JP1 event with event ID `2016` is issued).

An erroneous action wraps around in the action information file during action status monitoring (JP1 event with event ID `2021` is issued).

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

`COMMAND=`*command*

Specifies the notification command that is to be executed when an error is detected during automated action status monitoring.

You can execute the following types of commands:

When the host executing the command is Windows:

• Executable file (`.com`, `.exe`)

• Batch file (`.bat`)

• JP1/Script script file (`.spt`)

(An appropriate association must have been set so that an `.spt` file can be executed.)

When the host executing the command is UNIX:

• Executable file (with execution permissions)

• Shell script (with execution permissions)

• If neither of the above applies or there is no definition, the default value `unspecified` is assumed.

The following notes apply to defining a notification command:

• Everything from `COMMAND=` to the linefeed code is defined as a single command.

• The maximum length of a command is 1,023 bytes.

If the character string obtained by expanding variables exceeds 1,023 bytes, the command will not execute.

In such a case, the message `KAVB4409-E` is output to the integrated trace log.

• The maximum length in bytes includes spaces, but does not include the linefeed code.

• If you specify a variable, specify it immediately after `$`. For details about the variables that can be specified, see *Table 2-19 Variables that can be specified in the automatic action notification definition file*.

The notification command specified in `COMMAND` inherits the execution environment of JP1/IM - Manager.

- The notification command is executed with the execution permissions of JP1/IM - Manager (Windows: SYSTEM user; UNIX: root).
- Specify in COMMAND the full path of the notification command.
- Specify for a notification command a command that will always terminate. If you set a batch file (Windows) or a shell script (UNIX), make sure that it will terminate with exit 0. If the specified command does not terminate or uses the GUI, processes of the executed notification command will remain unresolved.
- To use $, specify $$.

[DELAY_WATCH]

Defines whether an automated action error that is detected during automated action delay monitoring is to be notified by issuing a JP1 event or by executing a notification command.

EVENT={true | false}

Specifies whether a JP1 event (event ID: 2010) is to be issued when an error is detected during automated action delay monitoring.

Specify either true or false. If you wish to issue a JP1 event when an error is detected, specify true; otherwise, specify false. The default is true. When true is specified, a JP1 event (event ID: 2015 or 2020) is also issued in the following cases:

- Suppression of notification to the action delay monitoring function is released (JP1 event with event ID 2015 is issued).
- The erroneous action wraps around in the action information file during action delay monitoring (JP1 event with event ID 2020 is issued).

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

COMMAND=*command*

Specifies the notification command that is to be executed when an error is detected during automated action delay monitoring.

You can execute the following types of commands:

When the host executing the command is Windows:

- Executable file (.com, .exe)
- Batch file (.bat)
- JP1/Script script file (.spt)

(An appropriate association must have been set so that an .spt file can be executed.)

When the host executing the command is UNIX:

- Executable file (with execution permissions)
- Shell script (with execution permissions)
- If neither of the above applies or there is no definition, the default value unspecified is assumed.

The following notes apply to defining the notification command:

- Everything from COMMAND= to the linefeed code is defined as a single command.
- The maximum length of a command is 1,023 bytes.

If the character string obtained by expanding variables exceeds 1,023 bytes, the command will not execute.

In such a case, the message KAVB4409-E is output to the integrated trace log.

- The maximum length in bytes includes spaces, but does not include the linefeed code.
- If you specify a variable, specify it immediately after $. For details about the variables that can be specified, see *Table 2-19 Variables that can be specified in the automatic action notification definition file*.

The notification command specified in COMMAND inherits the execution environment of JP1/IM - Manager.

- The notification command is executed with the execution permissions of JP1/IM - Manager (Windows: SYSTEM user; UNIX: root).

- Specify in `COMMAND` the full path of the notification command.
- Specify for a notification command a command that will always terminate. If you set a batch file (Windows) or a shell script (UNIX), make sure that it will terminate with `exit 0`. If the specified command does not terminate or uses the GUI, processes of the executed notification command will remain unresolved.
- To use `$`, specify `$$`.

Table 2–19: Variables that can be specified in the automatic action notification definition file

Variable name	Description
`ACTSEQNO`	Serial number of the action that was placed in delayed or error status. When status monitoring is specified and the action in error status wraps around in the action information file, `(----)` is displayed.
`EVID`	Event ID of the action triggering event that was placed in delayed or error status (*basic-code* (8 hexadecimal characters)`:` *extended-code* (8 hexadecimal characters)). If the action that was placed in delayed or error status wraps around in the action information file, `(----:----)` is displayed.
`EVARVTIME`	Event arrival time (*YYYY*`/`*MM*`/`*DD* *hh*`:`*mm*`:`*ss*) of the action triggering event that was placed in delayed or error status. If the action that was placed in delayed or error status wraps around in the action information file, `(----/--/-- --:--:--)` is displayed.
`ACTSTAT`	Action status of the action that was placed in delayed or error status. One of the following character strings indicating the action execution status is displayed: • `running` (running) • `ended` (terminated) • `fail` (not executable) • `error` (execution failed) • `unknown` (status unknown) • `wait` (waiting for transmission) • `send` (transmitting) • `queue` (queuing) • `cancel` (canceled) • `kill` (terminated forcibly) If you cancel the action from JP1/IM - View, the cancellation status is displayed after the above status. While cancellation processing is underway: • `running(canceling)` • `send(canceling)` • `queue(canceling)` • `wait(canceling)` When cancellation processing failed: • `running(miss)` • `send(miss)` • `queue(miss)` • `wait(miss)` • `ended(miss)` • `error(miss)` If the command is re-executed when the Automatic Action Service is restarted or is output to the action re-execution file, the above status is suffixed with `-R` (example: `ended-R`). If the command is re-executed from JP1/IM - View, the above status is suffixed with `-RU` (example: `ended-RU`). If a suppressed action is re-executed from JP1/IM - View, the above status is suffixed with `-RUD` (example: `ended-RUD`).

Variable name	Description
	If a suppressed action is re-executed from JP1/IM - View and then re-executed again due to a restart (including system switching) of the Automatic Action Service during re-execution processing, or is output to the action re-execution file, the above status is suffixed with `-RD` (example: `ended-RD`). If a suppressed action is placed in `fail` status (not executable), the above status is suffixed with `-D` (example: `fail-D`). If delay monitoring is used and a delayed action wraps around in the action information file, `(----)` is displayed. If status monitoring is used and the action placed in error status wraps around in the action information file, one of the following character strings is displayed: • `fail` (not executable) • `error` (execution failed)
`ACTSTARTTIME`	Action start time of the action that was placed in delayed status (*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*). This time is displayed only when delay monitoring is used. If status monitoring is used, (`----/--/-- --:--:--`) is displayed. If delay monitoring is used and the delayed action wraps around in the action information file, `(----/--/-- --:--:--)` is displayed.
`ACTENDTIME`	Action end time of the action that was placed in error status (*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*). This time is displayed only when status monitoring is used. If delay monitoring is used, (`----/--/-- --:--:--`) is displayed. If status monitoring is used and the action that was placed in error status wraps around in the action information file, `(----/--/-- --:--:--)` is displayed.
`ACTHOST`	Execution host name for the action that was placed in delayed or error status. If delay monitoring is used and the delayed action wraps around in the action information file, `(----)` is displayed. If status monitoring is used and the action issued by an action definition in which *execution-host-name* is not specified is placed in `Fail` status, `(----)` is displayed.
`ACTUSR`	JP1 user name executing the action that was placed in delayed or error status. This is the user name registered at the execution host. If delay monitoring is used and the delayed action wraps around in the action information file, `(----)` is displayed. If status monitoring is used and the action issued by an action definition in which *execution-host-name* is not specified is placed in `Fail` status, `(----)` is displayed.

Example definition

This example issues a JP1 event and executes the notification command `statenotice01.exe` (for status monitoring) or `delaynotice01.exe` (for delay monitoring) when an error is detected during status monitoring or delay monitoring of automated actions:

```
[STATE_WATCH]
EVENT=true
COMMAND=C:\Command\statenotice01.exe
[End]
[DELAY_WATCH]
EVENT=true
COMMAND=C:\Command\delaynotice01.exe
[End]
```

File that defines which items are displayed for event conditions (attr_list.conf)

Format

```
# comment-line
attribute-name
attribute-name
attribute-name
   .
   .
   .
attribute-name
```

File

`attr_list.conf` (file that defines which items are displayed for event conditions)

`attr_list.conf.model` (model file for the file that defines which items are displayed for event conditions

Storage directory

In Windows

For a physical host:

Console-path`\conf\action\attr_list`

For a logical host:

shared-folder`\jp1cons\conf\action\attr_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/action/attr_list`

For a logical host:

shared-directory`/jp1cons/conf/action/attr_list`

Description

This file defines the items to be displayed in the **Attribute name** field in the Action Parameter Detailed Definitions window. The Action Parameter Detailed Definitions window displays the items in the **Attribute name** field in the order they are specified in this file.

When the definitions are applied

The file that defines which items are displayed for event conditions is loaded when Central Console is started or when the `jco_spmd_reload` command is executed. When JP1/IM - View displays the Action Parameter Definitions window, it acquires the contents of the file that defines the items and which was loaded by Central Console, and then applies the file's contents to the Action Parameter Detailed Definitions window.

Information that is specified

attribute-name

Specifies an item to be displayed in the **Attribute name** field of the Action Parameter Detailed Definitions window. Specify the attribute name of each item that is to be displayed with one item per line. You can specify from 0 to 256 items.

An attribute name is case sensitive. Any space or tab character immediately preceding or following the attribute name will be ignored.

The table below lists the attribute names that can be specified.

If you specify `SEPARATOR`, a horizontal line, such as `--------------------`, is displayed in the **Attribute name** field of the Action Parameter Detailed Definitions window. You can use `SEPARATOR` to separate the items that are used often from the items that are used infrequently.

If you specify only `SEPARATOR`, only a horizontal line is displayed in the **Attribute name** field. In such a case, no event condition can be set by selecting the separator line and then adding an event condition.

Table 2–20: List of items that can be displayed

No.	Display item	Attribute name
1	Source host	`B.SOURCESERVER`
2	Event level	`E.SEVERITY`
3	Object type	`E.OBJECT_TYPE`
4	Object name	`E.OBJECT_NAME`
5	Root object type	`E.ROOT_OBJECT_TYPE`
6	Root object name	`E.ROOT_OBJECT_NAME`
7	Occurrence	`E.OCCURRENCE`
8	User name	`E.USER_NAME`
9	Message	`B.MESSAGE`
10	Product name	`E.PRODUCT_NAME`
11	Event ID	`B.ID`
12	Start time	`E.START_TIME`
13	End time	`E.END_TIME`
14	Registered time	`B.TIME`
15	Arrived time	`B.ARRIVEDTIME`
16	Program-specific extended attribute	`OTHER_EXTENDED_ATTRIBUTE`
17	Reason for registration	`B.REASON`
18	Source process ID	`B.PROCESSID`
19	Source user name	`B.USERNAME`
20	Source user ID	`B.USERID`
21	Source group name	`B.GROUPNAME`
22	Source group ID	`B.GROUPID`
23	Source IP address	`B.SOURCEIPADDR`

No.	Display item	Attribute name
24	Object ID	E.OBJECT_ID
25	Result code	E.RESULT_CODE
26	Event source host name	E.JP1_SOURCEHOST
27	Basic event information	B.BASIC
28	Detailed event information	B.DETAIL
29	--------------------	SEPARATOR

Note:

If an attribute name has already been specified, subsequent specifications of the same name are ignored.

If the event display item definition file could not be read and the number of valid display items is zero, items 1 through 25 are displayed.

#*comment-line*

A line beginning with a hash mark (#) is treated as a comment.

Example definition

```
B.SOURCESERVER
E.SEVERITY
E.OBJECT_TYPE
E.OBJECT_NAME
E.ROOT_OBJECT_TYPE
E.ROOT_OBJECT_NAME
E.OCCURRENCE
E.USER_NAME
B.MESSAGE
E.PRODUCT_NAME
B.ID
E.START_TIME
E.END_TIME
B.TIME
B.ARRIVEDTIME
OTHER_EXTENDED_ATTRIBUTE
B.REASON
B.PROCESSID
B.USERNAME
B.USERID
B.GROUPNAME
B.GROUPID
B.SOURCEIPADDR
E.OBJECT_ID
E.RESULT_CODE
E.JP1_SOURCEHOST
```

Configuration file for converting information (event_info_replace.conf)

Format

```
character-before-conversion=character-string-after-conversion
character-before-conversion=character-string-after-conversion
      :
character-before-conversion=character-string-after-conversion
```

File

`event_info_replace.conf`

Storage directory

In Windows

For a physical host:

Console-path`\conf\action`

For a logical host:

shared-folder`\jp1cons\conf\action`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/action`

For a logical host:

shared-directory`/jp1cons/conf/action`

File permissions

The following permissions are needed to use the configuration file for converting information:

In Windows

The Administrators group and `SYSTEM` users must be able to reference the file.

In UNIX

Users with the `root` permissions must be able to reference the file.

Description

This file specifies the following conversion rules:

- Conversion rules for the event takeover information transform function of the auto action and command execution.
- Conversion rules of string for suggestion activation condition and response action when type is `cmd` in suggestion function.
- Conversion rules of string for auto response action and manual response action when type is `cmd`

The above string can convert certain ASCII characters in event-takeover information to another string according to conversion rules of configuration file for converting information.

For details about suggestion activation criteria with type `cmd` and response action strings in the suggestion function, see *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.

For details on when type `cmd` in auto response action, see the section *Automatic execution of response actions* of *Chapter 7. Automatic execution and manual execution of response action (JP1/IM - Agent linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

For details on when type `cmd` in manual response action, see the section *Manual execution of response actions* of *Chapter 7. Automatic execution and manual execution of response action (JP1/IM - Agent linkage)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The configuration file for converting information is not created when JP1/IM - Manager is installed. To use this configuration file, use a text editor to create and edit `event_info_replace.conf`.

When the definitions are applied

For an automated action:

The contents of the configuration file for converting information take effect when JP1/IM - Manager starts, when the **Apply** button is clicked on the Action Parameter Definitions window of JP1/IM - View, and when the `jcachange` command is executed to reload the definition.

For command execution:

The contents of the configuration file for converting information take effect when the Execute Command window opens.

For the Intelligent Integrated Management Base (suggestion function, auto and manual execution function in Response Action):

The contents of the configuration file for converting information take effect when the JP1/IM3-Manager service is started, when the `jddupdatesuggestion` command is executed to reload the suggestion definition, or when REST API is execute to load the auto response action definition.

If loading the configuration file for converting information fails when the JP1/IM3-Manager service is started, conversion is made with no conversion rule.

If loading the configuration file for converting information fails when the `jddupdatesuggestion` command is executed to load the suggestion definition, or when REST API is execute to load the auto response action definition, conversion is made with the conversion rules before the suggestion definition is loaded.

Note that if there is no configuration file for converting information, the function works without any conversion rule.

Information that is specified

character-before-conversion=character-string-after-conversion

Define in the configuration file for converting information conversion rules for the event inheritance information conversion function. Each rule consists of a *character-before-conversion* and a *character-string-after-conversion*. You can specify from 0 to 34 conversion rules.

Lines consisting of only spaces, tabs, or linefeed codes in the event inheritance information conversion settings file are ignored. Specify one conversion rule per line. Separate the character before conversion from the character string after conversion with an equal sign (=).

A defined line that is not in the format *character-before-conversion=character-string-after-conversion* is ignored and processing continues. If no character string after conversion is specified, the function assumes that the specified character before conversion is to be deleted from the event inheritance information.

There can be only one conversion rule for the same character before conversion. If more than one conversion rule is specified for the same character before conversion, the first conversion rule specified takes effect and the subsequent conversion rules for that character are ignored.

If the event inheritance information contains a control character (`0x01` to `0x08`, `0x0A` to `0x1F`, or `0x7F`), the control character is converted to a space (`0x20`).

If either of the following applies, the conversion rules are ignored and processing continues:

- A character that cannot be specified as a character before conversion is specified.
- Two or more characters are specified as a character before conversion.

character-before-conversion

As a character before conversion, you can specify an ASCII character (`0x00` to `0x7F`) indicated by *Y* in the applicable *character-before-conversion* column of the table below.

The table below lists the ASCII characters that can be specified as the character before conversion.

Table 2–21: Characters that can be specified as a character before conversion and a character string after conversion

Character	Hexadecimal value	*character-before-conversion*	*character-string-after-conversion*
Control character	`0x00 to 0x08`	N	N
Tab	`0x09`	Y	Y
Control character	`0x0a to 0x1f`	N	N
Space	`0x20`	Y	Y
`!`	`0x21`	Y	Y
`"`	`0x22`	Y	Y
`#`	`0x23`	Y	Y
`$`	`0x24`	Y	Y
`%`	`0x25`	Y	Y
`&`	`0x26`	Y	Y
`'`	`0x27`	Y	Y
`(`	`0x28`	Y	Y
`)`	`0x29`	Y	Y
`*`	`0x2a`	Y	Y
`+`	`0x2b`	Y	Y
`-`	`0x2c`	Y	Y
`.`	`0x2d`	Y	Y
`/`	`0x2e`	Y	Y
`:`	`0x2f`	Y	Y
`;`	`0x3b`	N	Y
`<`	`0x3c`	Y	Y
`=`	`0x3d`	Y	Y
`>`	`0x3e`	Y	Y
`?`	`0x3f`	Y	Y
`@`	`0x40`	Y	Y

Character	Hexadecimal value	*character-before-conversion*	*character-string-after-conversion*
[	0x5b	Y	Y
\	0x5c	Y	Y
]	0x5d	N	Y
^	0x5e	Y	Y
_	0x60	Y	Y
{	0x7b	Y	Y
|	0x7c	Y	Y
}	0x7d	Y	Y
~	0x7e	Y	Y

Legend:

Y: Can be specified

N: Cannot be specified

character-string-after-conversion

As a character string after conversion, you can specify 0 to 2 ASCII characters (0x00 to 0x7F) indicated by *Y* in the applicable *character-string-after-conversion* column of the above table.

Example definition

The following shows examples of converting ", ', and * to _:

```
"=_
'=_
*=_
```

When the value for a message (B.MESSAGE) receives a JP1 event, The Web server goes down. Details: "NetworkΔError", the value for the entire message text (variable: EVMSG) will be The Web server goes down. Details: _NetworkΔError_.

Extended startup process definition file (jp1co_service.conf)

Format

```
process-name|startup-options|whether-restartable|restart-count|retry-interva
l|restart-count-reset-time|
```

File

`jp1co_service.conf` (extended startup process definition file)

`jp1co_service.conf.model` (model file for the extended startup process definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\`

For a logical host:

shared-folder`\jp1cons\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/`

For a logical host:

shared-directory`/jp1cons/conf/`

Description

This file defines process information for the functions that constitute JP1/IM - Manager.

JP1/IM - Manager uses the process management function to control restart in the event of abnormal termination of a process. The process management function controls processes according to the definition in the extended startup process definition file.

Do not specify in this file any unneeded characters, such as spaces. Edit numeric values for only those parameters on which editing is permitted.

Customize only the applicable parameters as appropriate to your operations. Normally, there is no need to change the settings for other parameters because appropriate values have already been set in them as the default values for each process.

In the case of a cluster configuration, if the extended startup process definition file is not found in the `conf` folder for the logical host when the a process management process is started at the logical host, the extended startup process definition file for the physical host is copied.

When the definitions are applied

The contents of the definition file take effect when JP1/IM - Manager starts or when the `jco_spmd_reload` command is executed to reload the definition. A change in the *startup-options* parameter takes effect only when JP1/IM - Manager starts.

Information that is specified

process-name

Specifies the name of a process that is to be started and terminated by the process management function of JP1/IM - Manager.

JP1/IM - Manager's process name is already specified, and must not be edited.

The name specified here must be a process name displayed by the `jco_spmd_status` command.

startup-options

Specifies startup options for the process.

`-Xmx`

The `-xmx` parameter is a parameter that sets the maximum size of the Java heap space.

The size of the heap area used by the `evtcon` process and the `jddmain` process might exceed the initial value, depending on user settings. The `evtcon` process defaults to `-Xmx 512m`, with a default size of 512 megabytes. The `jddmain` process has no default specification, and the default size is 8,192 megabytes.

If the estimated heap area size that is required exceeds default value, you must change the `-Xmx` parameter's value to a value after a estimation.

For details about how to estimate the heap area size, see the Release Notes for JP1/IM - Manager.

Notes about startup options

- If you change the heap area size for the `evtcon` process of JP1/IM - Manager, check by performing appropriate tests that the change will not cause problems. Even if the value is within the permissible range for the heap area size, a memory shortage might occur and JP1/IM - Manager might terminate or information might not be updated in the Event Console window, resulting in unstable operation. If this occurs, revise as necessary the **Event buffer** and **Num. of events to acquire in 1 search** settings by referencing the formula for estimating the heap area size.
- The maximum memory size cited in the Release Notes for JP1/IM - Manager is a logical value. It might not be possible to allocate the set heap area depending on the OS, the environment in use, and the applications that run concurrently. If the heap area cannot be allocated or the set value is less than default value, problems might occur, such as a JP1/IM - Manager startup error.

The following example changes the heap area size of the `evtcon` process from 512 to 1,024 megabytes in Windows:

Example:

Before the heap area size is changed to 1,024 megabytes (from an initial size of 512 megabytes):

```
evtcon|-Xmx512m|0|3|3|3600|
```

After the heap area size has been changed to 1,024 megabytes:

```
evtcon|-Xmx1024m|0|3|3|3600|
```

whether-restartable

Specifies whether the process is to be restarted if it terminates abnormally.

Specify `0` to not restart the process and `1` to restart the process.

The default is 0.

restart-count

Specifies the number of times process restart is to be attempted.

The permitted value range is from 0 to 99. The default is 3.

Note that if `0` is specified in the *whether-restartable* field, this field is ignored even if a value is specified.

retry-interval

Specifies in seconds the interval between process restart attempts.

The permitted value range is from 0 to 3,600. The default is 3.

Note that if 0 is specified in the *whether-restartable* field, this field is ignored even if a value is specified.

restart-count-reset-time

Specifies in seconds the amount of time that is to elapse before the restart count will be reset after the process has restarted.

The permitted value range is from 3,600 to 2,147,483,647 (seconds). The default is 3,600.

The restart count is reset when the specified amount of time has elapsed after the process has restarted. If the process terminates abnormally again after this amount of time has elapsed, the restart count starts again from 1. If the process terminates abnormally again within the specified amount of time after it has restarted, the previous restart count is inherited.

Note that if 0 is specified in the *whether-restartable* field, this field is ignored even if a value is specified.

Example definition

The following shows an example of an extended startup process definition file:

```
evflow||0|3|3|3600|
jcamain||0|3|3|3600|
evtcon|-Xmx512m|0|3|3|3600|
evgen||0|3|3|3600|
jcsmain||0|3|3|3600|
jcfmain||0|3|3|3600|
jddmain||0|3|3|3600|
imbase||0|3|3|3600|
imbaseproxy||0|3|3|3600|
```

IM parameter definition file (jp1co_param_V7.conf)

Format

```
[logical-host-name\JP1CONSOLEMANAGER]
"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:value
"SEND_PROCESS_RESTART_EVENT"=dword:value
```

File

`jp1co_param_V7.conf` (IM parameter definition file)

`jp1co_param_V7.conf.model` (model file for the IM parameter definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\`

For a logical host:

shared-folder`\jp1cons\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/`

For a logical host:

shared-directory`/jp1cons/conf/`

Description

This file defines whether a JP1 event is to be issued when JP1/IM - Manager processes fail or when JP1/IM - Manager processes are recovered automatically from abnormal termination. The following lists the JP1/IM - Manager processes and the JP1 events that can be issued.

- JP1/IM - Manager processes
  - Event Console Service (`evtcon`)
  - Event Base Service (`evflow`)
  - Automatic Action Service (`jcamain`)
  - Central Scope Service (`jcsmain`)
  - Event Generation Service (`evgen`)
- JP1 events that can be issued
  - JP1 event whose event ID is `3F90`: This event can be issued when a process terminates abnormally.
  - JP1 event whose event ID is `3F91`: This event can be issued when a timeout occurs during process startup.
  - JP1 event whose event ID is `3F92`: This event can be issued when a process that terminated abnormally has successfully completed restart processing.

By issuing a JP1 event when a process recovers automatically from a process error or abnormal termination, you can manage the history of JP1/IM - Manager failures. For this reason, we recommend that you use this definition file to set issuance of such JP1 events.

The required definitions are provided as a model file. To change the settings, copy the model file and then edit the copy.

When the definitions are applied

The contents of the file take effect when JP1/IM - Manager is restarted by execution of the `jbssetcnf` command with this definition file specified in an argument.

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER]`

Specifies the key name for the JP1/IM - Manager environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:`*value*

When `1` is set in *value*, a JP1 event is issued in the following cases:

- A process terminates abnormally (JP1 event whose event ID is `3F90` is issued).
- A timeout occurs during startup processing without a startup notification (JP1 event whose event ID is `3F91` is issued).

The default is `0`, in which case no JP1 event is issued.

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

`"SEND_PROCESS_RESTART_EVENT"=dword:`*value*

When `1` is set in *value*, a JP1 event is issued in the following case:

- Restart processing of a process that terminated abnormally is completed successfully (JP1 event whose event ID is `3F92` is issued).

The default is `0`, in which case no JP1 event is issued.

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

Example definition

```
[JP1_DEFAULT\JP1CONSOLEMANAGER]
"SEND_PROCESS_TERMINATED_ABNORMALLY_EVENT"=dword:0
"SEND_PROCESS_RESTART_EVENT"=dword:0
```

Make sure that the end of the file is at the beginning of the last line.

System profile (.system)

Format

```
DESC_VERSION=15
     :
[ServerDefine]
InvalidateTime = 1440
EventCount = event-buffer-count
Debug = true
[End]
     :
[RetryInfo]
RetryCount = retry-count
RetryInterval = retry-interval
[End]
```

File

`.system` (system profile)

`.system.model` (model file for the system profile)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\profile\`

For a logical host:

shared-folder`\jp1cons\conf\console\profile\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/profile/`

For a logical host:

shared-directory`/jp1cons/conf/console/profile/`

Description

This file defines the basic operation of the event console.

There is a system profile for each manager (JP1/IM - Manager). The file defines information about the system environment for the event console (such as the number of event buffers and a retry count for connecting to the event service during event search). The information defined in this profile affects all instances of JP1/IM - View that are connected to the manager to which this profile is applicable.

When the definitions are applied

The definition takes effect when JP1/IM - Manager starts or when the **Apply** button is clicked in the System Environment Settings window.

Information that is specified

`EventCount = ` *event-buffer-count*

Specifies the maximum number of events that can be buffered at the manager when events are extracted from the event service.

The permitted value range is from 10 to 2,000. The default is 2,000.

`RetryCount = ` *retry-count*

Specifies the maximum number of times automatic connection establishment can be retried after connection with the event service has failed or the connection has been lost during event search.

The permitted value range is from 0 to 100. The default is 3.

`RetryInterval = ` *retry-interval*

Specifies in milliseconds the retry interval between attempts to establish connection after connection with the event service has failed or the connection has been lost during event search.

The permitted value range is from 1 to 86,400,000. The default is 10,000.

Notes

- Specify the settings in the System Environment Settings window, unless otherwise necessary.
- Be attentive to the values that you set because the contents of the system profile affect all event console operations. Do not change any attribute or attribute value that is not explained here. If such an attribute or attribute value is changed, the event console might not function correctly.
- You must terminate JP1/IM - View before you edit the system profile.
- There is one system profile for each manager. Therefore, if you have changed the manager for logging in, you must change the system profile at the connection destinations.
- When you intend to edit the contents of the `.system` file, we recommend that you make a backup before editing the file.
- If the system profile contains an error, such as an attribute value that is outside the permitted range of values, the event console might not function correctly.

Example definition

```
DESC_VERSION=15
    :
[End]
[ServerDefine]
InvalidateTime = 1440
EventCount = 500
Debug = true
[End]
    :
[RetryInfo]
RetryCount = 3
RetryInterval = 10000
[End]
[LocaleInformation]
Language=English
[End]
```

User profile (defaultUser | profile_user-name)

Format

```
DESC_VERSION=file-version
[DisplayItemContainer]#
    :
[DisplayItemInformation]
ValidTab=All
Visible=whether-visible
AttrName=JP1-event-attribute-name
AttrOrder=sort-order
ColumnSize=column-width
[End]
[End]
    :
```

#: You can edit only placeholders in italic placed in a section that is enclosed with `[DisplayItemInformation]` and `[End]` and that includes `ValidTab=All`.

File

`defaultUser` (default user profile)

`defaultUser.model` (model file for the default user profile)

`profile_`*user-name* (user profile for an individual JP1 user)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\profile\`

For a logical host:

shared-folder`\jp1cons\conf\console\profile\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/profile/`

For a logical host:

shared-directory`/jp1cons/conf/console/profile/`

Description

This file defines environment information about how the Event Console window is displayed for each user.

At the manager, there is a user profile for each user. A user profile defines a user environment for the event console (principally, environment information about the window display). A user profile can be created for each user under the name `profile_`*user-name* (using the JP1 user's user name). There is also a default profile, `defaultUser`, that can be used as the default profile for any user. If you edit the `defaultUser` profile, the new contents become the default profile for user profiles that are created in the future.

You can define `profile_`*user-name* in the Preferences window. If there are any errors in the user profile, the Event Console window might not display correctly. For this reason, we recommend that you use the Preferences window of JP1/IM - View to define user profiles.

When the definitions are applied

The definition takes effect the next time you log in to JP1/IM - Manager (Central Console).

Information that is specified

`DESC_VERSION=`*file-version*

Specifies the version of the user profile being created. The items that can be specified in `[DisplayItemInformation]` to `[End]` depend on the value specified for the file version. For program version 11-00 or later, specify `15` as the file version. If the file version specified is `11` or earlier, do not attempt to change the file version.

The following operations update all instances of `profile_`*user-name* to the most recent file version:

- Saving the Preferences window from JP1/IM - View
- Saving the column width of the items that are displayed in the list of events on a page in the Event Console window during logout from JP1/IM - View

To set `defaultUser` (default user profile) to file version 12, overwrite `defaultUser` with `defaultUser.model` (model file for the default user profile), and then edit the file.

`[DisplayItemInformation]` to `[End]`

Specify the attributes of JP1 events that are to be displayed in the Event Console window.

`[DisplayItemInformation]` through `[End]` constitute a single definition block. The contents of this definition block take effect on all three pages of the Event Console window. To add a definition block, insert it between `[DisplayItemContainer]` and `[End]`.

The parameters that can be specified in `[DisplayItemInformation]` through `[End]` are described below.

You must not edit the parameters in `[DisplayItemInformation]` through `[End]` for a definition block in which `AttrOrder=0` is specified, because such definition blocks are used by the system.

`ValidTab = All`

This is a fixed character string that must not be changed.

`Visible =` *whether-visible*

Specifies whether the information for the attribute specified in `AttrName` is to be displayed. If `true` is specified in *whether-visible*, information about the attribute specified in `AttrName` is displayed. If `false` is specified, information about the attribute specified in `AttrName` is not displayed. When `false` is specified, the corresponding item is displayed in **Available items** in the Preferences window. If you specify `false`, you must specify `-1` in `AttrOrder`.

`AttrName =` *attribute-name-to-be-displayed*

Specifies the attribute name of the JP1 event. Information about the attribute specified here is displayed in the Event Console window.

The following table lists the attributes that can be set.

Table 2–22: List of attributes that can be set in attribute-name-to-be-displayed

No.	Specifiable attribute name	Attribute	DESC_VERSION			
			1-10[#1]	11	12-14	15
1	`IM.EVENT_TYPE`	Type	Y	Y	Y	Y

No.	Specifiable attribute name	Attribute	DESC_VERSION			
			1-10[#1]	11	12-14	15
2	B.SEQNO	Serial number	Y	Y	Y	Y
3	B.IDBASE	Event ID	Y	Y	Y	Y
4	B.PROCESSID	Source process ID	Y	Y	Y	Y
5	B.TIME	Registered time	Y	Y	Y	Y
6	B.ARRIVEDTIME	Arrived time	Y	Y	Y	Y
7	B.USERID	Source user ID	Y	Y	Y	Y
8	B.GROUPID	Source group ID	Y	Y	Y	Y
9	B.USERNAME	Source user name	Y	Y	Y	Y
10	B.GROUPNAME	Source group name	Y	Y	Y	Y
11	B.SOURCESERVER	Source host	Y	Y	Y	Y
12	B.SOURCESEQNO	Source serial number	Y	Y	Y	Y
13	B.MESSAGE	Message	Y	Y	Y	Y
14	E.SEVERITY	Event level	Y	Y	Y	Y
15	E.USER_NAME	User name	Y	Y	Y	Y
16	E.PRODUCT_NAME	Product name	Y	Y	Y	Y
17	E.OBJECT_TYPE	Object type	Y	Y	Y	Y
18	E.OBJECT_NAME	Object name	Y	Y	Y	Y
19	E.OBJECT_ID	Object ID	Y	Y	Y	Y
20	E.ROOT_OBJECT_TYPE	Root object type	Y	Y	Y	Y
21	E.ROOT_OBJECT_NAME	Root object name	Y	Y	Y	Y
22	E.OCCURRENCE	Occurrence	Y	Y	Y	Y
23	E.START_TIME	Start time	Y	Y	Y	Y
24	E.END_TIME	End time	Y	Y	Y	Y
25	E.@JP1IM_ACTCONTROL	Action	N	Y	Y	Y
26	E.@JP1IM_ACTTYPE	Action type	N	Y	Y	Y
27	E.@JP1IM_ORIGINAL_SEVERITY	Original severity level	N	Y	Y	Y
28	E.@JP1IM_CHANGE_SEVERITY	New severity level	N	Y	Y	Y
29	E.@JP1IM_DISPLAY_MESSAGE	Changed display message	N	N	N	Y
30	E.@JP1IM_CHANGE_MESSAGE	New display message	N	N	N	Y
31	E.@JP1IM_CHANGE_MESSAGE_NAME	Display message change definition	N	N	N	Y
32	E.@JP1IM_MEMO	Memo	N	Y	Y	Y
33	E.JP1_SOURCEHOST	Event source host name	N	N	Y	Y

No.	Specifiable attribute name	Attribute	DESC_VERSION			
			1-10#1	11	12-14	15
34	E.ACTION_TARGET#2	Action	Y	N	N	N
35	IM.ACTION_TYPE#2	Action type	Y	N	N	N
36	E.*	Program-specific extended attribute	N	N	N	Y

Legend:

Y: Can be specified

N: Cannot be specified

#1

There are no differences in the items that can be specified for file versions 1 through 10.

#2

These items are compatible with version 8. If `DESC_VERSION` is `10` or earlier (definition for version 8 or earlier), these attributes are converted as follows:

`E.ACTION_TARGET` → `E.@JP1IM_ACTCONTROL`

`IM.ACTION_TYPE` → `E.@JP1IM_ACTTYPE`

`AttrOrder =` *sort-order*

Specifies the display column location relative to the left margin. If you specify `1`, the attribute is displayed as the first (leftmost) item in the list of events. Do not specify the same value for more than one item.

Do not specify `0` because it is used by the system.

If there are any errors in the user profile, the Event Console window might not display correctly. For this reason, we recommend that you use the Preferences window of JP1/IM - View to define user profiles.

`ColumnSize =` *column-width*

Specifies the column width. The permitted value range is from 1 to 1,000.

Notes

- Specify each user profile carefully because the contents of this file affect overall event console operation. Do not change any attribute or attribute value that is not explained here. If such an attribute or attribute value is changed, the event console might not function correctly.
- Because a user profile might be overwritten during JP1/IM - View operation or termination processing, make sure that you terminate JP1/IM - View before editing a user profile.
- There is one user profile for each manager. Therefore, if you have changed the manager for logging in, you must change the profile at the connection destinations.
- When you intend to edit the contents of the `defaultUser` file, you must make a backup before editing the file.
- Using JP1/Base's user management to delete a user does not delete the user profile for that user.
- If you use JP1/Base's user management to rename a user, the user's existing user profile is not inherited.
- If a user profile contains an error, such as an attribute value outside the permitted range of values, the event console might not function correctly.

Communication environment definition file (console.conf.update)

Format

```
[logical-host-name\JP1CONSOLEMANAGER\EVCONS]
"COM_SO_TIMEOUT"=dword:hexadecimal-value

[JP1_DEFAULT\JP1CONSOLE_CMD]
"COM_SO_TIMEOUT"=dword:hexadecimal-value
"COM_RETRY_COUNT"=dword:hexadecimal-value
"COM_RETRY_INTERVAL"=dword:hexadecimal-value
"COM_RMI_TIMEOUT"=dword:hexadecimal-value
```

File

`console.conf.update` (model file for the communication environment definition file)

Storage directory

In Windows

Console-path`\default\`

In UNIX

`/etc/opt/jp1cons/default/`

Description

This file defines communication processing (timeout period) among JP1/IM - Manager, the viewer, and the `jcochstat` command.

When a low-speed line is used in the network for communication between the viewer and JP1/IM - Manager or when the viewer's workload is high, timeouts might occur during the viewer's communication processing, resulting in communication errors. You can prevent such communication errors by modifying the timeout period.

When the `jcochstat` command is used from another manager to change the action status of a JP1 event at the local host, a communication error might occur due to a timeout during communication processing. Modifying the timeout period and the connection retry count might resolve the problem, preventing a recurrence of the communication error.

If you are using JP1/IM - View (event console), you must also change the communication environment definition file for JP1/IM - View (event console) (`view.conf.update`).

The required definitions are provided as a model file. To change the settings, copy the model file and edit the copy after renaming the copy to definition file (for Windows: *console-path*`\conf\console.conf`, for UNIX: `/etc/opt/jp1cons/conf/console.conf`).

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER\EVCONS]`

Specifies the key name for Event Console Service environment settings.

For *logical-host-name*, specify JP1_DEFAULT for the physical host and *logical-host-name* for a logical host.

"COM_SO_TIMEOUT"=dword:*hexadecimal-value*

Specifies as a hexadecimal value the timeout period in milliseconds. The default value is dword:0000EA60 (60,000 milliseconds).

The range of values that can be specified is from 0x00000001 to 0x0036EE80 (3,600,000 milliseconds).

The specified value must not exceed the value specified for COM_RMI_TIMEOUT (default: 0000EA60) in the console.conf.update communication environment definition file and the view.conf.update communication environment definition file. Additionally, check the setting value (timeout period) on the connection source.

[JP1_DEFAULT\JP1CONSOLE_CMD]

Specifies the key name for the jcochstat command environment settings.

"COM_SO_TIMEOUT"=dword:*hexadecimal-value*

Specifies as a hexadecimal value the timeout period in milliseconds. The default value is dword:0000EA60 (60,000 milliseconds).

The range of values that can be specified is from 0x00000001 to 0x0036EE80 (3,600,000 milliseconds).

The specified value must not exceed the value specified for COM_RMI_TIMEOUT (default: 0000EA60) in the communication environment definition file (view.conf.update).

"COM_RETRY_COUNT"=dword:*hexadecimal-value*

Specifies as a hexadecimal value the retry count to be applied in the event of a communication error. The default is dword:00000003 (3 times).

The range of values that can be specified is from 0x00000001 to 0x7fffffff (2,147,483,647 times).

"COM_RETRY_INTERVAL"=dword:*hexadecimal-value*

Specifies as a hexadecimal value the wait time in milliseconds between retry attempts. The default is dword:00000BB8 (3,000 milliseconds).

The range of values that can be specified is from 0x00000001 to 0x7fffffff (2,147,483,647 milliseconds).

"COM_RMI_TIMEOUT"=dword:*hexadecimal-value*

Specifies as a hexadecimal value the timeout period in milliseconds for the event action status to change. The permitted value range is from 0000EA60 to 0036EE80 (from 60,000 to 3,600,000 milliseconds). The default is dword:0000EA60 (60,000 milliseconds).

If the KAVB1205-E message is displayed frequently, set a longer timeout period.

Example definition

```
[JP1_DEFAULT\JP1CONSOLEMANAGER\EVCONS]
"COM_SO_TIMEOUT"=dword:000009C4

[JP1_DEFAULT\JP1CONSOLE_CMD]
"COM_SO_TIMEOUT"=dword:0000EA60
"COM_RETRY_COUNT"=dword:00000003
"COM_RETRY_INTERVAL"=dword:00000BB8
```

Make sure that the end of the file is at the beginning of the last line.

Health check definition file (jcohc.conf)

Format

```
[HEALTHCHECK]
ENABLE={true | false}
FAILOVER={true | false}
EVENT={true | false}
COMMAND=command
NO_RESPONSE_TIME=no-response-time
ERROR_THRESHOLD=no-response-count-treated-as-error
BASE_NO_RESPONSE_TIME=no-response-time
BASE_ERROR_THRESHOLD=no-response-count-treated-as-error
[End]
```

File

`jcohc.conf` (health check definition file)

`jcohc.conf.model`(model file for the health check definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\health\`

For a logical host:

shared-folder`\jp1cons\conf\health\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/health/`

For a logical host:

shared-directory`/jp1cons/conf/health/`

Description

This file defines whether the health check function is to be enabled. If you enable the health check function, you can also define whether errors are to be notified by issuing a JP1 event or by executing a notification command.

You must specify this definition file by using the character encoding supported by JP1/IM - Manager.

If you have deleted the health check definition file (`jcohc.conf`), copy the model file for the health check definition file (`jcohc.conf.model`) under the name `jcohc.conf` and then edit the definition in the copy, if necessary.

The health check function cannot monitor Central Scope Service (`jcsmain`).

When you enable the health check function by using this definition file, you gain the capability to check whether each process of JP1/IM - Manager and the event service of JP1/Base on the local host is running normally.

The health check function can detect errors in the following processes:

- Event Console Service (`evtcon`)
- Automatic Action Service (`jcamain`)
- Event Base Service (`evflow`)
- Event Generation Service (`evgen`)
- Event service (`jevservice`)

If any of these processes hang up# or terminate abnormally, the health check function can issue a JP1 event or execute a specified notification command to prompt the operator to recover the process.

#

A process hang-up is a status in which a process can no longer accept processing requests due to deadlock or looping.

When the definitions are applied

The settings in the health check definition file take effect at the following times:

- When JP1/IM - Manager is started.
- When the file is reloaded by the `jco_spmd_reload` command.

Information that is specified

`ENABLE={true | false}`

Specifies whether the health check function is to be enabled.

Specify either `true` or `false`. To enable the health check function, specify `true`; to disable the function, specify `false`. The default is `false`.

When the health check function has been enabled and it detects an error, a message (`KAVB8060-E` or `KAVB8062-E`) is output to the integrated trace and the Windows event log (`syslog`) reporting whether the `EVENT` setting in the health check definition file is `true` or `false`.

`FAILOVER={true | false}`

Specifies whether a JP1/IM - Manager operation is to be performed when an error is detected by the health check function when you are operating in a cluster system. Specify `true` if the operation is to be performed, or specify `false` if the operation is not to be performed. The default is `false`. If you do not use a cluster system, do not change the default setting.

- In Windows

  When `true` is specified, JP1/IM - Manager is terminated when an error is detected. When the health check function detects an error, it notifies the cluster system of the error in JP1/IM - Manager by stopping JP1/IM - Manager. If you set the cluster system to fail over when a JP1/IM - Manager error occurs, failover can take place when an error is detected.

- In UNIX

  When `true` is specified, the JP1/IM - Manager process in which the error was detected is terminated. When the health check function detects an error, it notifies a cluster system of the error in JP1/IM - Manager by stopping JP1/IM - Manager. If you set the cluster system so that, on detection of an error, it is stopped forcibly by the `jco_killall.cluster` command and then failed over, failover can take place when an error is detected.

`EVENT={true | false}`

Specifies whether JP1 events (event ID: `2012` and `2013`) are to be issued when an error is detected by the health check function.

Specify either `true` or `false`. If JP1 events are to be issued, specify `true`; otherwise, specify `false`.

The default is `true`. When `true` is specified, a JP1 event (event ID: `2014`) is also issued in the following case:

- The health check function detects abnormal recovery.

For details about JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

`COMMAND=`*command*

Specifies the notification command that is to be executed when an error is detected by the health check function.

You can execute the following types of commands:

When the host executing the command is Windows:

- Executable file (`.com`, `.exe`)
- Batch file (`.bat`)
- JP1/Script script file (`.spt`)
  (An appropriate association must have been set so that an `.spt` file can be executed.)

When the host executing the command is UNIX:

- Executable file (with execution permissions)
- Shell script (with execution permissions)

The following notes apply to defining a notification command:

- Everything from `COMMAND=` to the linefeed code is defined as a single command.
- The maximum length of a command is 1,023 bytes. This length includes spaces, but does not include the linefeed code. If the length exceeds 1,023 bytes, the default value is assumed. If you specify variables and the character string obtained by expanding variables exceeds 1,023 bytes, the command will not execute. In such a case, the message `KAVB8072-E` is output to the integrated trace log.
- If you specify a variable, specify it immediately after `$`. The following table lists and describes the variables that can be specified.

Table 2–23: Variables that can be specified in notification commands

Variable name	Description
`HCHOST`	Name of host resulting in the error
`HCFUNC`	Name of function resulting in the error (`evflow`, `jcamain`, `evtcon`, `evgen`, or `jevservice`)
`HCPNAME`	Name of process resulting in the error (`evflow`, `jcamain`, `evtcon`, `evgen`, or `jevservice`)
`HCPID`	• For `evflow`, `jcamain`, `evtcon`, or `evgen` ID of process resulting in the error • For `jevservice` -1
`HCDATE`	Date the error occurred (*YYYY*/*MM*/*DD*)
`HCTIME`	Time the error occurred (*hh*:*mm*:*ss*)

- For the notification command, specify a command that will always terminate. If you set a batch file (Windows) or shell script (UNIX), make sure that it will terminate with `exit 0`. If the specified command does not terminate or uses the GUI, processes of the executed notification command will remain unresolved.
- The notification command specified in `COMMAND` inherits the execution environment of JP1/IM - Manager.

- The notification command is executed with the execution permissions of JP1/IM - Manager (Windows: `SYSTEM` user; UNIX: `root`).
- Specify in `COMMAND` the full path of the notification command.

Use the `jcohctest` command to test thoroughly whether the set notification command functions successfully. For details about the `jcohctest` command, see *jcohctest* in *1. Commands*.

- The default is `COMMAND=`, in which case no notification command is executed.
- To use `$`, specify `$$`.
- In Windows, if you execute a command in the `%WINDIR%\System32` folder, the WOW64 redirect functionality redirects execution to the same command in the `%WINDIR%\SysWow64` folder. If there is no applicable command in the destination folder, command execution might fail. Make sure that the applicable command is in the `%WINDIR%\System32` folder when you specify it for execution.

`NO_RESPONSE_TIME=`*no-response-time*

Specifies in seconds the amount of time to wait for a response to be sent from the JP1/IM - Manager process. The permitted value range is from 60 to 3,600 seconds. The default is 60 seconds.

If the value that is specified is outside the permitted value range or the definition is omitted, the default value (60 seconds) is assumed.

Note that this parameter is not included in the health check definition file (`jcohc.conf`) that is deployed when JP1/IM - Manager is installed. If you want to change the default value, you must add the parameter.

`ERROR_THRESHOLD=`*no-response-count-treated-as-error*

Specifies the number of times to wait for the set no-response time to elapse before assuming that an error has occurred in the JP1/IM - Manager process. The permitted value range is from 1 to 60 times. The default is 3 times.

If the value that is specified is outside the permitted value range or the definition is omitted, the default value (3 times) is assumed.

`BASE_NO_RESPONSE_TIME=`*no-response-time*

Specifies in seconds the interval for checking the JP1/Base event service for the set no-response time on Manager. The permitted value range is from 60 to 3,600 seconds. The default is 300 seconds.

If the value that is specified is outside the permitted value range or the definition is omitted, the default value (300 seconds) is assumed.

`BASE_ERROR_THRESHOLD=`*no-response-count-treated-as-error*

Specifies the number of times to wait for the set no-response time to elapse before assuming that an error has occurred in the JP1/Base event service on Manager. The permitted value range is from 1 to 60 times. The default is 2.

If the value that is specified is outside the permitted value range or the definition is omitted, the default value (2 times) is assumed.

Example definition

Issue a JP1 event and execute the `jcohc01.exe` notification command when an error is detected by the health check function:

```
[HEALTHCHECK]
ENABLE=true
FAILOVER=false
EVENT=true
COMMAND=C:\Command\jcohc01.exe
NO_RESPONSE_TIME=60
ERROR_THRESHOLD=3
BASE_NO_RESPONSE_TIME=300
```

```
BASE_ERROR_THRESHOLD=2
[End]
```

Event guide information file (jco_guide.txt)

Format

```
DESC_VERSION=file-version

[EV_GUIDE_event-guide-number]
EV_USER=JP1-user-name
EV_COMP=attribute-name:attribute-value
EV_GUIDE=event-guide-message
[END]
[EV_GUIDE_event-guide-number]
EV_COMP=attribute-name:attribute-value
EV_COMP=attribute-name:attribute-value
EV_FILE=event-guide-message-file-name
[END]
   :
```

File

`sample_jco_guide_ja.txt` (sample file of the event guide information file (Japanese))

`sample_jco_guide_en.txt` (sample file of the event guide information file (English))

`sample_jco_guide_ja.txt.model` (model file for the event guide information sample file (Japanese))

`sample_jco_guide_en.txt.model` (model file for the event guide information sample file (English))

Storage directory

In Windows

For a physical host:

Console-path`\conf\guide\`

For a logical host:

shared-folder`\jp1cons\conf\guide\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/guide/`

For a logical host:

shared-directory`/jp1cons/conf/guide/`

Description

This file defines event guide information for JP1 events. The information specified in this file is displayed in the Event Details window of JP1/IM - View or the Event Detail window of the integrated operation viewer.

The maximum size of an event guide information file is 1 megabyte. An event guide information file can contain up to 1,000 blocks.

Use the language encoding supported by JP1/IM - Manager to specify the event guide information file.

You must create an event guide information file under the name `jco_guide.txt`. Copy the `sample_jco_guide_ja.txt` or `sample_jco_guide_en.txt`, depending on the language code used by JP1/IM - Manager, and then rename the file `jco_guide.txt` before you use it. Store the event guide information file in the same directory that stores the sample file. Note that the event guide information file cannot have a user-selected name, unlike the file specified in the `EV_FILE` parameter (event guide message file).

If an issued JP1 event matches multiple event guide information items, the first item specified in the event guide information file is effective.

When # is specified, any text following # is treated as a comment. Note that a comment cannot be specified after the start tag, attribute information, or the end tag. An error results if a comment is specified following the start tag or the end tag. A comment that is specified following an attribute value is treated as part of the attribute value.

To use `\`, specify `\\`. If `\` is used in a character combination other than `\n` or `\$`, a log is output and the line containing `\` is ignored.

The event guide information file and event guide message file are not checked for HTML syntax errors.

When the definitions are applied

Once the event guide information file has been edited, the definitions in the file take effect when JP1/IM - Manager is restarted or when the `jco_spmd_reload` command is executed. If there is no display area for event guide information in the Event Details window when you log in to JP1/IM - View or the Event Detail window of the integrated operation viewer, apply the definitions and then re-log in to JP1/IM - View or the Event Detail window of the integrated operation viewer. The display area should appear.

After you have edited the event guide message file, you can display the new information by reloading the Event Details window.

Information that is specified

`DESC_VERSION=`*file-version*

Specifies the file version of the event guide information file. The specifiable values are `1` and `2`. When `2` is specified, you can specify the `EV_USER` parameter.

`[EV_GUIDE_`*event-guide-number*`]`

This is the start tag for event guide information. The information from the `[EV_GUIDE_`*event-guide-number*`]` to the `[END]` tag constitutes a single definition block. Between this parameter and `[END]`, specify a comparison condition for determining the JP1 events that are to be displayed in the Event Details window and the message to be displayed. For *event-guide-number*, specify a decimal number in the range from 1 to 9999.

When there are multiple definition blocks, the event guide numbers need not be in numerical order. However, an error results if the same event guide number is specified more than once, in which case the definition block with the duplicated event guide number is ignored. Note that `[EV_GUIDE_1]` and `[EV_GUIDE_0001]` are different.

Specify a unique character string in each `EV_GUIDE_`*event-guide-number*. If an invalid character string is specified, a log is output and the corresponding specification is ignored.

If an attribute specified for `EV_GUIDE_`*event-guide-number* is not permitted, the corresponding specification is ignored.

`EV_USER=`*JP1-user-name*

Specifies the JP1 user name to be displayed in the event guide message. You can specify 1 to 31 bytes of characters. Only one-byte alphanumeric characters can be used. Alphabetic characters are not case sensitive. If you specify this parameter, specify `2` for `DESC_VERSION`. You can specify this parameter only once. If the parameter is omitted, all JP1 users are assumed as applicable users.

This parameter can be specified only when the version of JP1/IM - Manager is 09-50 or later. You can specify a maximum of 100 JP1 user names by separating them with one or more spaces.

Example:

```
EV_USER=jp1user1 jp1user2 jp1user3
```

`EV_COMP=`*attribute-name*`:`*attribute-value*

Specify this parameter for each attribute that is to be used for comparison with JP1 events. When multiple attributes are specified, they are assumed to be connected by the AND condition. For example, if the `EV_COMP` parameter is specified twice, the event guide message is displayed in the Event Details window only when both of the conditions are satisfied.

If you specify an event ID for the attribute name in an `EV_COMP` parameter, you can specify either `B.ID` or `B.IDBASE`. In `B.ID`, specify the 16-digit attribute value in the format *basic-part*`:`*extended-part*. In `B.IDBASE`, specify the 8-digit basic part.

Example:

- `EV_COMP=B.ID:00004107:00000000`
- `EV_COMP=B.IDBASE:00004107`

You can specify a maximum of 100 `EV_COMP` conditions. For an example of using more than one `EV_COMP` condition, see the example definition below.

Note that a business group name cannot be used for the event-issuing server name (`B.SOURCESERVER`), the target event server name (`B.DESTSERVER`), and the event source host name (`E.JP1_SOURCEHOST`). If you specify a business group name, it is treated as a host name.

attribute-name

Specifies one of the following as the attribute:

• JP1 event basic attribute: If you specify this attribute, use the format `B.`*attribute-name*.

• JP1 event extended attribute: If you specify this attribute, use the format `E.`*attribute-name*.

Note that the reason for registration (`B.REASON`) and code set (`B.CODESET`) cannot be specified.

If you specify the registration time (`B.TIME`) or the arrival time (`B.ARRIVEDTIME`) for *attribute-name*, the total number of milliseconds after UTC January 1, 1970 at 00:00:00 is compared.

Example: Specify a JP1 event of which the arrival time is 10:20:00.000 (total number of milliseconds: 1371000000000) on June 12, 2013

```
EV_COMP=B.TIME:1371000000000
```

attribute-value

Specifies as a regular expression the value of the attribute specified in *attribute-name*. For the regular expression, use an extended regular expression. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

By default, the specified regular expression is compared with the entire attribute value of the JP1 event. The condition is satisfied only if they match exactly.

To accept a partial match, execute the `jbssetcnf` command specifying a file that contains the common definition information shown below in an argument and then restart JP1/IM - Manager to apply the definition. When you create the definition file, make sure that the end of the file is at the beginning of the last line.

For a physical host

```
[JP1_DEFAULT\JP1CONSOLEMANAGER]
"GUIDE_EV_COMP"="find"
```

For a logical host

```
[logical-host-name\JP1CONSOLEMANAGER]
"GUIDE_EV_COMP"="find"
```

To reset the definition to a complete match (default), specify `match` for the value of the `GUIDE_EV_COMP` common definition information.

If the common definition information is missing or the specified value is invalid, the system assumes `match` for a complete match.

Note that the common definition information is not set at the time of installation.

When you specify an IPv6 address for a source IP address (`B.SOURCEIPADDR`) and the target IP address (`B.DESTIPADDR`), use lowercase alphabetic characters as in the following example:

```
0011:2233:4455:6677:8899:aabb:ccdd:eeff
```

Also note that abbreviated IP addresses such as the following cannot be specified:

```
2012:7:8::a:b
```

When you specify the registered time (`B.TIME`) or the arrived time (`B.ARRIVEDTIME`), specify the number of seconds in milliseconds starting from UTC 1970-01-01 00:00:00.

`EV_GUIDE=`*event-guide-message*

Specifies a character string that is to be displayed as the event guide information. The specified character string is displayed in the event guide information area in the Event Details window (in **Guide** under **Message**).

Note that you can specify this parameter only once between `[EV_GUIDE_`*event-guide-number*`]` and `[END]`.

If you specify `EV_GUIDE=`*event-guide-message* and `EV_FILE=`*event-guide-message-file-name* together, the specification of `EV_FILE=`*event-guide-message-file-name* takes precedence.

To use `\` in the message, specify `\\`. To use `$`, specify `\$`. To use a linefeed code in the message, specify `\n`.

You can use HTML tags and specify variables for JP1 event attributes in *event-guide-message*.

- Specifying HTML tags

  If you use HTML tags, you can display the event guide message in HTML format in the Event Details window (for details about the HTML tags that can be specified, see *Table 2-27 HTML tags that can be used in the event guide message file*, in the description of `EV_FILE`.

- Specifying variables for JP1 event attributes

  If you specify `$B.`*attribute-name*Δ or `$E.`*attribute-name*Δ in the message, the attribute value corresponding to the JP1 event attribute name is expanded in the message (Δ indicates a space). Note that the reason for registration (`B.REASON`) and code set (`B.CODESET`) cannot be specified. If there is no corresponding attribute, the attribute is replaced with blanks.

  The table below lists the attribute names that can be specified in messages. For details about the attributes of JP1 events, see *3.1 Attributes of JP1 events*.

Table 2–24: List of attribute names that can be specified in messages

JP1 event attribute		Specification in message
Basic attributes	Serial number	`B.SEQNO`
	Event ID	Specify either of the following: 1. `B.ID` 2. `B.IDBASE`
	Source process ID	`B.PROCESSID`
	Registered time	`B.TIME`
	Arrived time	`B.ARRIVEDTIME`
	Source user ID	`B.USERID`
	Source group ID	`B.GROUPID`
	Source user name	`B.USERNAME`

JP1 event attribute		Specification in message
	Source group name	`B.GROUPNAME`
	Event-issuing server name	`B.SOURCESERVER`
	Target event server name	`B.DESTSERVER`
	Source serial number	`B.SOURCESEQNO`
	Message	`B.MESSAGE`
Extended attributes	Event level	`E.SEVERITY`
	User name	`E.USER_NAME`
	Product name	`E.PRODUCT_NAME`
	Object type	`E.OBJECT_TYPE`
	Object name	`E.OBJECT_NAME`
	Root object type	`E.ROOT_OBJECT_TYPE`
	Root object name	`E.ROOT_OBJECT_NAME`
	Object ID	`E.OBJECT_ID`
	Occurrence	`E.OCCURRENCE`
	Start time	`E.START_TIME`
	End time	`E.END_TIME`
	Result code	`E.RESULT_CODE`
	Event source host name	`E.JP1_SOURCEHOST`
	Other extended attribute	`E.`*xxxxxx*#

#:

You can also specify JP1 product-specific extended attributes. For example, the product-specific extended attribute for the JP1/AJS job execution host is `E.C0`. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

You can specify for an event guide message a maximum of 196,608 characters. If more than 196,608 characters are specified, the portion in excess of 196,608 characters will not be displayed in the Event Details window.

The event guide message can display a Web page of related products without unreadable text by specifying replacement characters listed in the table below.

Table 2–25: Replacement characters that can be specified

Specification format	Description
`$B.`*attribute-name*Δ `$E.`*attribute-name*Δ	Expand the attribute value as is. When guide information is in HTML format, use HTML encoding. Specify the attribute value in this format to display the JP1 event attribute value as part of the text to be displayed in an event guide message. Example: `$B.MESSAGEΔ`

`$B.`*attribute-name*`$URLENCΔ`
`$E.`*attribute-name*`$URLENCΔ`
	Handle the attribute value as a UTF-8 string for URL encoding and expand it.
	Use this format to pass the JP1 event attribute value as a UTF-8 string to be used as the argument (URL parameter) of the Web page application.
	Example: `<a href="http://host/page?msg=$B.MESSAGE$URLENCΔ">`

`$B.`*attribute-name*`$ENCΔ`
`$E.`*attribute-name*`$ENCΔ`
	Perform Base64 encoding for the attribute value as a UTF-8 string and expand it.
	Use this format to display the Base64-encoded JP1 event attribute value as a UTF-8 string as part of the text to be displayed in an event guide message.

Specification format	Description
	However, to pass the value as an argument (URL parameter) of a Web page application, use the variables `$B.`*attribute-name*`$ENC$URLENC`Δ, `$E.`*attribute-name*`$ENC$URLENC`Δ Example: `$B.MESSAGE$ENC`Δ
`$B.`*attribute-name*`$ENC$URLENC`Δ `$E.`*attribute-name*`$ENC$URLENC`Δ	Perform Base64 encoding for the attribute value as a UTF-8 string, and then perform URL-encoding to expand it. Use this format to pass the Base64 value of the JP1 event attribute value as an argument (URL parameter) of the Web page application. Example: `<a href="http://host/page?msg=$B.MESSAGE$ENC$URLENC`Δ`">`

Note:

When you specify `$URLENC` or `$ENC`, you must specify `2` as the value for `DESC_VERSION`.

`EV_FILE=`*event-guide-message-file-name*

Specifies the full path name of a file that contains the text for the event guide message that is to be displayed in the Event Details window. You can specify this parameter only once between `[EV_GUIDE_`*event-guide-number*`]` and `[END]`. If nothing is specified for *event-guide-message-file-name*, the file names in the following table are assumed.

Table 2–26: Event guide message file name

OS	Event guide message file name
Windows	*Console-path*`\conf\guide\EV_GUIDE_`*event-guide-number*`.txt`
	shared-folder`\jp1cons\conf\guide\EV_GUIDE_`*event-guide-number*`.txt`
UNIX	`/etc/opt/jp1cons/conf/guide/EV_GUIDE_`*event-guide-number*`.txt`
	shared-directory`/jp1cons/conf/guide/EV_GUIDE_`*event-guide-number*`.txt`

Express the file name using from 1 to 1,024 characters, including the path. If the specified file name exceeds 1,024 characters, an error results when JP1/IM - Manager starts or when the event guide message file is called from JP1/IM - View or the integrated operation viewer.

You can specify any file name and extension for the event guide message file. We recommend that you select a file name that is easy to manage; for the extension, use `.txt` if the event guide message is in TXT format and `.html` or `.htm` if the event guide message is in HTML format.

Example: `jco_guidemes001_AJS2.txt` or `jco_guidemes001_AJS2.htm`

Event guide message file

Specify in the event guide message file in TXT or HTML format the information that you want to be displayed in the Event Details window. The information that you can specify in the event guide information file is the same as for `EV_GUIDE`. In other words, you can use HTML tags and variables for the attributes of JP1 events. To use a backslash sign (`\`) in a message, write it as`\\`. To use the dollar sign (`$`), write it as`\$`. To insert a linefeed in a message, write it as`\n`.

However, `EV_GUIDE` can be used only to specify a one-line message, whereas with the event guide message file you can use linefeed codes for a formatted message.

You can store the created event guide message file in any folder.

The maximum size of an event guide message file is 1 megabyte. If the file size exceeds 1 megabyte, an error occurs when the event guide message file is loaded into the Event Details window of JP1/IM - View or the integrated operation viewer.

The table below lists and describes the HTML tags and attributes that can be used when you create an event guide message file in HTML format. If any other HTML tags are used, the operational results cannot be guaranteed.

Table 2–27: HTML tags that can be used in the event guide message file

Tag	Attribute	Description
HTML	--	Declares that this is an HTML text. This tag is mandatory.
HEAD	--	Declares the header for the HTML text. This tag is mandatory.
BODY	--	Declares the body of the HTML text. This tag is mandatory.
A[#1]	HREF="*URL*"	Specifies a linkage-target URL.[#2, #3] You can specify URLs beginning with http:// or https://. Operation with other URLs is unpredictable. The link specified here is displayed in the Event Details window (HTML format). Clicking the link starts a Web browser and accesses the specified URL. You can encode a maximum of 2,083 characters.
	TARGET[#5]	Specifies the name of the destination window for the page indicated by the URL specified in HREF. If a destination window with the same name is found in the range of the same session as that of the WWW browser displaying the Integrated Operation Viewer, the window is used as a display destination. If the destination window is not found, a new window is opened and used as the display destination. This attribute can accept the following characters: • Half-width upper-case and lower-case alphabetic characters • Half-width numbers • Space characters • Symbols (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~) Note that the string cannot start with a half-width number, a space character, or a symbol. However, when you specify _blank, you can specify _ as the first letter. The names below are not available. It is case-insensitive. • _parent • _self • _top • Name that starts with JP1IM_ • Name with zero length, such as target=""
H1, H2, H3, H4, H5, H6	--	Specifies headers.
FONT	SIZE="*font-size*"	Specifies the font size. The permitted values are from 1 to 7.
	COLOR="*font-color*"	Specifies the font color. You can specify the following 16 colors: black, silver, gray, white, maroon, red, purple, fuchsia, green, lime, olive, yellow, navy, blue, teal, aqua If you specify any other font color, the operation is not guaranteed.
B	--	Specifies boldface type.
I[#4]	--	Specifies italics type.
HR	--	Specifies a horizontal rule.
BR	--	Specifies a forced linefeed.

Legend:

--: None

#1: The interpretation of the URL in the `A` tag and the screen to be displayed are dependent on the WWW browser and other aspects of the environment.

#2: The following is a coding example of a URL used to link with JP1/Navigation Platform.

Example:

```
http://hostA:8080/ucnpBase/portal/screen/Home/action/
PLoginUser?contentId=f24077e7-0136-1000-8000-00000ad20b6f-0
```

For details about linking with JP1/Navigation Platform, see the descriptions of the URL for calling Navigation Platform from JP1 products in the JP1/Navigation Platform manuals.

#3: For details about the URL for linking with JP1/AJS, see the JP1/AJS manuals.

#4: In the integrated operation viewer window, Japanese strings are not italicized even with the `I` tag.

#5: This attribute is available only for the Integrated Operation Viewer window.

`[END]`

Specifies the end tag for the event guide information. This item is not case sensitive.

Example definition

```
# JP1/IM-CC Guide Information File.

DESC_VERSION=1
[EV_GUIDE_001]
EV_COMP=B.ID:00004107:00000000
EV_COMP=E.SEVERITY:Error
EV_GUIDE=The job terminated abnormally.\nCheck whether an error has occurre
d on the $E.C0 host.
[END]
```

System color definition file (systemColor.conf)

Format

```
DESC_VERSION=file-version

#comment-line
[DEFAULT.BackgroundColor=color]
[DEFAULT.TextColor=color]

[SEVERITY.event-level.BackgroundColor=color]
[SEVERITY.event-level.TextColor=color]
:
```

File

`systemColor.conf` (system color definition file)

`systemColor.conf.model` (model file for the system color definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\profile`

For a logical host:

shared-folder`\jp1cons\conf\console\profile`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/profile`

For a logical host:

shared-directory`/jp1cons/conf/console/profile`

Description

This file defines the color settings used on the **Monitor Events** page, **Severe Events** page, and **Search Events** page of the Event Console window.

Execution permission

In Windows

The Administrators group and `SYSTEM` users must be able to reference the file.

In UNIX

Users with the `root` permissions must be able to reference the file.

When the definitions are applied

When you select the **Display** check box in the **Coloring** section of the Preferences window, the events in an event list are colored according to the settings specified in the system color definition file.

JP1/IM - View colors the events according to the settings in the system color definition file specified when the user logs in.

If a user changes the settings in the system color definition file during the login process, the new settings take effect when the user restarts JP1/IM - View.

Information that is specified

`DESC_VERSION=`*file-version*

Indicates the system color definition file format version. The value to be specified is `1`. If this value is omitted or another numeric value is specified, `1` is assumed.

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

`[DEFAULT.BackgroundColor=`*color*`]`

Specifies the default background color. If the background color for the event level is not specified, or is specified for a JP1 event that does not match the specification of the background color, the background color specified for this parameter is applied. This parameter can be omitted. The background color is specified by the name of the color or by RGB values. The following table shows the correspondence between color name and RGB values.

Color name	RGB value
`black`	`0,0,0`
`blue`	`0,0,255`
`cyan`	`0,255,255`
`darkGray`	`64,64,64`
`gray`	`128,128,128`
`green`	`0,255,0`
`lightGray`	`192,192,192`
`magenta`	`255,0,255`
`orange`	`255,200,0`
`pink`	`255,175,175`
`red`	`255,0,0`
`white`	`255,255,255`
`yellow`	`255,255,0`

The color names are not case sensitive.

The range of RGB values that can be specified is from 0 to 255. The default value is `white` (`255,255,255`). RGB values are separated by a comma (`,`).

`[DEFAULT.TextColor=`*color*`]`

Specifies the text color of an event level if a color is not specified. This parameter can be omitted. The color name, the RGB values, and the range of RGB values are the same as `DEFAULT.BackgroundColor=`*color*. The color names are not case sensitive.

The default value is `black` (`0,0,0`).

[SEVERITY.*event-level*.BackgroundColor=*color*]

Specifies the background color of an event level. This parameter can be omitted. The color name, the RGB values, and the range of RGB values are the same as DEFAULT.BackgroundColor=*color*. The color names are not case sensitive.

The event levels that can be specified are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug. The event levels are case sensitive.

[SEVERITY.*event-level*.TextColor=*color*]

Specifies the text color of the event level. This parameter can be omitted. The color name, the RGB values, and the range of RGB values are the same as DEFAULT.BackgroundColor=*color*. The color names are not case sensitive.

The event levels that can be specified are Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug. The event levels are case sensitive.

Example definition

```
DESC_VERSION=1

DEFAULT.TextColor=black
DEFAULT.BackgroundColor=white

SEVERITY.Emergency.TextColor=white
SEVERITY.Emergency.BackgroundColor=red

SEVERITY.Alert.TextColor=white
SEVERITY.Alert.BackgroundColor=red

SEVERITY.Critical.TextColor=white
SEVERITY.Critical.BackgroundColor=red

SEVERITY.Error.TextColor=white
SEVERITY.Error.BackgroundColor=255,128,0

SEVERITY.Warning.TextColor=black
SEVERITY.Warning.BackgroundColor=yellow
```

Definition file for extended event attributes

Format

```
@encode character-encoding
@file type="definition-file-type", version="definition-format-version";
@product name="product-name";
@define-block type="event-attr-def";
block lang = "language-type", platform="platform-type"
attr name="attribute-name", title="display-item-name"[, type="attribute-disp
lay-type"];
...
@define-block-end;
@define-block type="event-attr-group-def";
block platform="platform-type"
group name="group-name", attrs="list-of-attribute-names";
...
@define-block-end;
@define-block type="event-attr-order-def";
block platform="platform-type"
order id="event-ID-definition-character-string", attrs="list-of-attribute-na
mes";
...
@define-block-end;
```

File

The extension of a definition file for extended event attributes must be `.conf` (in lowercase).

`default.conf` (default definition file for extended event attributes)

`hitachi_`*xxxx*`.conf` (definition file for extended event attributes for a linked product)

company-name_product-name`_attr.conf` (user-defined definition file for extended event attributes)

company-name can be changed to *series-name_product-name*. We recommend that you use the value specified for `PRODUCT_NAME` at the time of JP1 event issuance as the file name, with the forward slash (`/`) replaced by the underscore (`_`). Because, `hitachi` is used for the default file name, use a name other than `hitachi` for *company-name*.

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\attribute\`

For a logical host:

shared-folder`\JP1Cons\conf\console\attribute\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/attribute/`

For a logical host:

shared-directory`/jp1cons/conf/console/attribute/`

Description

A definition file for extended event attributes defines the order for sorting the event attributes and the attribute names that are to be displayed in the Event Details window.

The following table describes the four types of definition files for extended event attributes.

Table 2–28: Types of definition files for extended event attributes

No.	Type	Description
1	Default file	Definition of detailed event information about the basic attributes common to all events and the common information of extended attributes
2	Extended file	Definition of program-specific extended attributes
3	File provided by a linked product	Definition of program-specific information about the extended attributes of a linked product that issues JP1 events
4	User-defined file	User-specific information about user-defined extended attributes

The two file types listed under No. 1 and No. 3 above are stored in the definition file storage directory of JP1/IM. These two types of files are system standard definition files created when JP1/IM - Manager is installed, and they cannot be added to, changed, or deleted by the user.

To add new user- or program-specific information about extended attributes of JP1 events, you can create a definition file of type No. 2 or No. 4 above and store it in the storage directory.

For details about file type No. 2, see *Definition file for extended event attributes (extended file)* in *Chapter 2. Definition Files*.

Creation timing

The following shows when the different types of definition files for extended event attributes are created.

No.	File type	When created
1	`default.conf`	When JP1/IM - Manager is installed
2	`hitachi_`*xxxx*`.conf`	When JP1/IM - Manager is installed
3	*company-name_product-name*`_attr.conf`	When the user adds the file

When the definitions are applied

The definitions in the definition file for extended event attributes take effect after either of the following occurs:

- JP1/IM - Manager is restarted.
- The command `jco_spmd_reload` is executed.

Information that is specified

A definition file for extended event attributes defines the order for sorting event attributes and the attribute names that are to be displayed in the Event Details window of JP1/IM - View or the Event Detail window of the integrated operation viewer.

There are three types of definition files for extended event attributes:

- File for definition of detailed event information about the basic attributes common to all events and the common information for extended attributes (file included with the product: `default.conf`)
- File for definition of program-specific information about the extended attributes of a linked product that issues JP1 events (file included with the product: `hitachi_`*`xxxx`*`.conf`)
- File for definition of user-specific information about user-defined extended attributes (created by the user)

The definition files for extended event attributes that are created when JP1/IM - Manager is installed are system standard definition files, and they cannot be added to, changed, or deleted by the user.

To add new user-specific information about extended attributes of JP1 events, you can create a definition file according to the naming rules described in *Table 2-2 Naming rules for definition files* and then store the file in the same definition file storage directory.

You should note the following about creating such a definition file:

- In JP1/IM - Manager for Linux, use UTF-8 encoding. In JP1/IM - Manager for OSs other than Linux, use Shift-JIS or EUC encoding.
  - If you mistakenly define the basic attributes or common information for the extended attributes in the definition file, the following is displayed if attributes (attribute name, item name, and attribute display type) are duplicated.
  - If only the attribute name or item name is duplicated: The attribute names and item names defined in each definition file are displayed.
  - If all attributes are duplicated: Specifications of the default file (`default.conf`) for the definition files for extended event attributes are ignored.

JP1/IM provides the `jcoattrfcheck` command for checking the contents of a definition file for extended event attributes. For details about this command, see *jcoattrfcheck* in *Chapter 1. Commands*.

You can specify the statements and blocks described in the table below in a definition file for extended event attributes.

Table 2–29: Statements and blocks that can be specified in a definition file for extended event attributes

Statement or block	Description
`@encode` statement	Specifies the character encoding used in the definition file
`@file` statement	Declares the definition file type and version
`@product` statement	Declares product information in the definition
Definition block for extended event attributes	Defines the display of event attributes
Definition block for attribute groups	Defines event attribute groups
Definition block for the attribute display order	Defines ID the order in which attributes are displayed in the Event Details window

Information that is specified (specification of character encoding)

`@encode`

Specifies the character encoding that is to be used in the definition file for extended event attributes. The `@encode` statement can be omitted.

To create an additional file for definition file for extended event attributes, use an @encode statement to specify the character set for the definition file.

Item names are expressed in characters that can be represented in the character encoding specified in the `@encode` statement. In addition, the definition file for extended event attributes is stored in the character encoding specified in the `@encode` statement.

In the following circumstances, item names displayed in JP1/IM - View or the integrated operation viewer might be garbled:

- If the item name uses characters that cannot be represented in the character encoding specified in the `@encode` statement
- If the character encoding specified in the `@encode` statement does not match the character encoding in which the file was saved

If no @encode statement exists or if there is an error in the specified character set name that follows the @encode statement, the character set is determined automatically. However, depending on the content of the definition file, the character encoding might not be determined correctly.

The following character encodings can be specified:

- C
- EUCJIS
- SJIS
- UTF-8
- GB18030

Note

If you use UTF-8 as the encoding to save a definition file, save the file without attaching a BOM (byte order mark).

An error is output in the following cases:

- A character encoding other than C, EUCJIS, SJIS, UTF-8 or GB18030 is specified
- The definition file does not begin with `@encode`.
- `@encode` is not followed by a character encoding value.

Note

If you use a definition file for extended event attributes provided by another product, make sure that the character encoding specified in the `@encode` statement matches the character encoding used in the definition file. In addition, if you plan to transfer definition files, do not convert their character encoding.

Information that is specified (rules for generating in-file statements)

`@file` *statement*

Declares that this is a definition file for extended event attributes and that the version of the definition specification format is 0300. This statement is mandatory.

This statement must be on the first line of the file, or on the line following the `@encode` statement. If the statement is not specified on the first line, the integrity of operations cannot be guaranteed.

Syntax

```
@file type="extended-attributes-definition", version="0300";
```

`@product` *statement*

Defines product information for the statements defined in the file.

When you specify this statement, note the following:

- The specified value must match the `PRODUCT_NAME` JP1 event extended attribute. If this specification is omitted, the integrity of operations cannot be guaranteed.

- Prohibited characters and formatting irregularities are not checked during parsing; instead, the specified character string is used as is.

Syntax

`@product name="`*product-name*`";`

`name="`*product-name*`"`

The product name is a string of alphanumeric characters separated by a forward slash. It must be specified in one of the following formats:

- /*company-name*/*series-name*/*product-name*
- /*company-name*/*product-name*

Example definition

The following shows an example of definition information header statements:

```
@file type="extended-attributes-definition", version="0300";
@product name="/HITACHI/JP1/CentralConsole";
@define-block type="event-attr-def";
block lang="English", platform="NT";
attr name="E.SAMPLE_TIME", title="Sample time";
attr name="E.SAMPLE_HOST", title="Sample host";
attr name="E.SAMPLE_USER", title="Sample user";
@define-block-end;
```

Information that is specified (rules for generating blocks in the definition file for extended event attributes)

This subsection describes the blocks that can be specified in a definition file for extended event attributes. If an invalid statement is specified in a block, an error is output but only the statement with the error is ignored.

Definition block for extended event attributes

In the Event Details window, associate the event attribute name with its display item name (for all Japanese, English, and Chinese names). You can specify this block more than once in the definition file unless the blocks have the same key attribute (the value specified in the `block` statement discussed below).

When specifying multiple languages, if you specify an attribute name in an `attr` statement (described below) for any one language, you must specify that attribute name in an `attr` statement for every specified language.

Types of statements that can be specified

You can specify the following statements in this block:

- `block` statement
- `attr` statement

Definition block for attribute groups

This block groups event attributes that are defined in the definition blocks for extended event attributes. If you group multiple event attributes, you can avoid defining `order` statements repeatedly in the definition blocks for the attribute display order.

This block is optional.

Types of statements that can be specified

You can specify the following statements in this block:

- `block` statement
- `group` statement

Definition block for the attribute display order

Defines the order in which event attributes and attribute names are to be displayed when the details of each event are displayed.

Types of statements that can be specified

You can specify the following statements in this block:

- `block` statement
- `order` statement

Information that is specified (rules for generating statements in a definition block for extended event attributes)

`block` statement

Defines block attributes. You can specify this statement only once at the beginning of a block.

Syntax

`block lang=`*language-type*`, platform=`*platform-type*`;`

`lang=`*language-type*

Declares the language used for the definition block for extended event attributes. You can specify one of the following languages:

- `Japanese`

Indicates that this is a definition for a Japanese language environment.

- `English`

Indicates that this is a definition for an English language environment.

- `Chinese`

Indicates that this is a definition for a Chinese language environment.

`platform=`*platform-type*

Specifies the platform to which the definition in the block is to be applied. You can specify the following values:

- `base`

The definition is applicable to all platforms.

If `base` is specified for the `platform` parameter, you must specify a comma (`,`) followed by `extended="false"`.

- *user-defined*

The definition is applicable to a user-defined platform. You must specify for *user-defined* a character string of alphanumeric characters. Note that this character string is not checked for errors.

The platform name specified in the `platform` parameter is compared with the `PLATFORM` JP1 event extended attribute; if they match, the specified information is subject to detailed information processing. If the platform name specified here is not found in the `PLATFORM` JP1 event extended attribute, the specified information is not processed. Note that if the `PLATFORM` extended attribute is not set at the time of JP1 event issuance, the system assumes that `base` is specified and executes file parsing.

Example definition

See the example definition for the `attr` statement below.

`attr` statement

Specifies an item name that is to be displayed in the attribute name column in the Event Details window and the type of the attribute value. You can specify this statement more than once in a block.

Note that this statement can be used to define only user-specific extended attribute information; the basic attributes and the common information of extended attributes are excluded. If the specified information is not user-specific extended attribute information, processing continues without outputting an error, but the specified information is displayed together with the provided standard definition information. For details about the standard definitions included with the product, see *Example definition* below.

Syntax

```
attr name=attribute-name, title=display-item-name[,type="elapsed_time/
date_format:CLIENT"];
```

`name=`*attribute-name*

Specifies the name of an attribute.

The following table lists the attributes that can be displayed.

No.	Specification format	Meaning of attribute
1	"B.SEQNO"	Serial number
2	"B.IDBASE"	Event ID
3	"B.PROCESSID"	Source process ID
4	"B.TIME"	Registered time
5	"B.ARRIVEDTIME"	Arrived time
6	"B.USERID"	Source user ID
7	"B.GROUPID"	Source group ID
8	"B.USERNAME"	Source user name
9	"B.GROUPNAME"	Source group name
10	"B.SOURCESERVER"	Source host
11	"B.DESTSERVER"	Target event server name
12	"B.SOURCESEQNO"	Source serial number
13	"B.MESSAGE"	Message
14	"B.SOURCEIPADDR"	Source IP address
15	"E.*extended-attribute-name*"	Extended attribute

`title=`*display-item-name*

Specifies the character string that is to be displayed in the attribute name column in the Event Details window; the language specified in the `block` statement will be used.

`type="elapsed_time/date_format:CLIENT"`

Specifies the type and display format of the attribute value. The attribute value `elapsed_time` is a decimal character string indicating the elapsed time in seconds since UTC 1970-01-01 00:00:00. The display format `date_format:CLIENT` means that the value is to be displayed in the time format by using the time specified in the local time zone of the target viewer.

Example definition

This subsection presents an example of user-specific extended attribute information for JP1 events. This is an example of a definition block for extended event attributes that displays four extended attributes (user-specific information) listed in the following table for the platform `W2K`.

Table 2–30: Example definition of a definition block for extended event attributes

Name displayed in the window	Extended attribute name (user-specific information)
`SAMPLE common attribute 1`	`COMMON_ATTR1`
`SAMPLE common attribute 2`	`COMMON_ATTR2`
`SAMPLE start attribute 1`	`START_ATTR1`
`SAMPLE start attribute 2`	`START_ATTR2`

```
@define-block type="event-attr-def";
block lang="English", platform="w2k";
attr name="E.COMMON_ATTR1",    title="SAMPLE common attribute 1";
attr name="E.COMMON_ATTR2",    title="SAMPLE common attribute 2";
attr name="E.START_ATTR1",     title="SAMPLE start attribute 1";
attr name="E.START_ATTR2",     title="SAMPLE start attribute 2";
@define-block-end;
```

Information that is specified (rules for generating statements in a definition block for attribute groups)

`block` statement

Defines block attributes. You can specify this statement only once at the beginning of a block.

When you define this statement, note the following:

- This block cannot contain the `lang` parameter.

Syntax

`block platform=`*platform-type*`;`

`platform=`*platform-type*

Specifies the platform to which the definition in the block is to be applied. You can specify the following values:

Specifiable value	Description
`"base"`	Use the value to enable the definition for all platforms. If `base` is specified for the `platform` parameter, you must specify a comma (`,`) followed by `extended="false"`.
`"`*user-defined*`"`	The definition is enabled for a user-defined platform. You must specify for *user-defined* a one-byte alphanumeric character string. Note that this character string is not checked for errors.

The platform name specified in the `platform` parameter is compared with the `PLATFORM` JP1 event extended attribute; if they match, the specified information is subject to detailed information processing. If the platform name specified here is not found in the `PLATFORM` JP1 event extended attribute, the specified information is not processed. Note that if the `PLATFORM` extended attribute is not set at the time of JP1 event issuance, the system assumes that `base` is specified and executes file parsing.

Example definition

See the example definition for the `group` statement below.

`group` statement

Groups attributes by assigning a name to a list of attributes that are to be displayed in the Event Details window. You can specify this statement more than once in a block.

Syntax

`group name=`*group-name*`, attrs=`*list-of-attribute-names*`;`

`name=`*group-name*

Specifies a name for the list of attribute names. Express the name using from 1 to 32 alphanumeric characters. This name is not case sensitive. You can use this name in the `order` block in the definition file.

`attrs=`*list-of-attribute-names*

Specifies a list of one or more attributes that are to be grouped. When multiple attributes are listed in this parameter, they are displayed in the Event Details window in the order specified here. The specification format is as follows:

- To specify only one attribute: `attrs="E.A0"`
- To specify multiple attributes: `attrs="E.A0|E.A1"`

Note that you can specify only user-specific extended attribute information. If you have specified a basic attribute or a common information item for an extended attribute, the specified attribute value is displayed more than once in the Event Details window.

Example definition

This example shows the definitions of basic attributes and user-specific information for JP1 event extended attributes. These definitions are provided as standard in the definition file for extended event attributes.

```
@define-block type="event-attr-group-def";
block platform="base", extended="false";
group name="BASE", attrs="B.GROUPID|B.GROUPNAME|B.IDBASE|B.PROCESSID|B.
SEQNO|B.SOURCEIPADDR|
B.SOURCESEQNO|B.SOURCESERVER|B.TIME|B.USERID|B.USERNAME|B.ARRIVEDTIME";
group name="COMMON", attrs="E.SEVERITY|E.USER_NAME|E.PRODUCT_NAME|E.OBJ
ECT_TYPE|E.OBJECT_NAME|
E.ROOT_OBJECT_TYPE|E.ROOT_OBJECT_NAME|E.OBJECT_ID|E.OCCURRENCE|
E.START_TIME|E.END_TIME|E.RESULT_CODE";
@define-block-end;
```

Information that is specified (rules for generating statements in a definition block for the attributes display order)

`block` statement

Defines the block attribute that depends on the definition block for the attribute display order. You can specify this statement only once at the beginning of a block.

When you define this statement, note the following:

- This block cannot contain the `lang` parameter.

Syntax

`block platform=`*platform-type*`;`

`platform=`*platform-type*

Specifies the platform to which the definition in the block is to be applied. You can specify the following values:

Table 2–31: Specifiable platforms

Specifiable value	Description
`"base"`	Use the value to enable the definition for all platforms. If `base` is specified for the `platform` parameter, you must specify a comma (`,`) followed by `extended="false"`.

Specifiable value	Description
"*user-defined*"	The definition is enabled for a user-defined platform. You must specify for *user-defined* a one-byte alphanumeric character string. Note that this character string is not checked for errors.

The platform name specified in the `platform` parameter is compared with the `PLATFORM` JP1 event extended attribute; if they match, the specified information is subject to detailed information processing. If the platform name specified here is not found in the `PLATFORM` JP1 event extended attribute, the specified information is not processed. Note that if the `PLATFORM` extended attribute is not set at the time of JP1 event issuance, the system assumes that `base` is specified and executes file parsing.

Example definition

See the example definition for the `order` statement below.

`order` statement

Defines by ID the attributes to be displayed in the Event Details window and their sort order. You can specify this statement more than once in a block.

Syntax

`order id=`*event-ID-definition-character-string*`, attrs=`*list-of-attribute-names*`;`

`id=`*event-ID-definition-character-string*

Specifies one event ID for which attributes are to be displayed in the order specified in the `attrs` parameter.

The specification format is as follows:

`id="200"`

Express an event ID using from 1 to 8 hexadecimal characters. If a specified event ID consists of fewer than 8 characters, there is no need to add leading zeros to pad it out to 8 characters. The alphabetic characters in the hexadecimal character string (`a` to `f`) are not case sensitive.

A range of IDs cannot be specified.

`attrs=`*list-of-attribute-names*

Specifies a list of the attributes, the groups, or both that are to be displayed. When multiple items are specified in this parameter, they are displayed in the Event Details window in the order specified here.

The specification format is as follows:

- To specify only one item: `attrs="E.A0"`
- To specify multiple items: `attrs="E.A0|E.A1|GROUP1"`

As is the case with the `group` statement, you can specify only user-specific extended attributes. If you have specified a basic attribute or common extended attribute, the specified attribute value will be displayed more than once in the Event Details window.

Example definition

This example definition displays the `BASE` and `COMMON` groups for event ID `00001000`:

```
@define-block type="event-attr-order-def";
block platform="base", extended="false";
order id="00001000", attrs="BASE|COMMON"
@define-block-end;
```

Example definition of a definition file for extended event attributes

```
@encode UTF-8
@file type="extended-attributes-definition", version="0300";
@product name="/HITACHI/JP1/SAMPLE";
```

```
@define-block type="event-attr-def";
block platform="base", lang="English", extended="false";
attr name="E.SAMPLE_CLUSTER_NAME", title="Cluster name";
attr name="E.SAMPLE_PRINT_SERVER_NAME", title="Print server name";
attr name="E.SAMPLE_PRINTER_NAME", title="Printer name";
attr name="E.SAMPLE_PORT_NAME", title="Port name";
@define-block-end;
@define-block type="event-attr-group-def";
block platform="base", extended="false";
group name="_PRINTER_INFO",
attrs="E.SAMPLE_PRINT_SERVER_NAME|E.SAMPLE_PRINTER_NAME";
group name="_CLUSTER_INFO", attrs="E.SAMPLE_CLUSTER_NAME|E.SAMPLE_PORT_NAME
";
@define-block-end;
@define-block type="event-attr-order-def";
block platform="base", extended="false";
order id="00003100",attrs="_PRINTER_INFO";
order id="00003101",attrs="_CLUSTER_INFO";
order id="00003102", attrs="_PRINTER_INFO|_CLUSTER_INFO";

@define-block-end;
```

Definition file for extended event attributes that is included with the product

Shown below are the definitions of the basic attributes and the common information for extended attributes for JP1 events. These definitions are included with the product as the definition file for extended event attributes.

```
@define-block type="event-attr-def";
block lang="English", platform="base", extended="false";
attr name="B.SEQNO",             title="Serial number";
attr name="B.IDBASE",            title="Event ID";
attr name="B.PROCESSID",         title="Source process ID";
attr name="B.TIME",              title="Registered time", type="elapsed_time_
in_milli/date_format:CLIENT";
attr name="B.ARRIVEDTIME",       title="Arrival time", type="elapsed_time/dat
e_format:CLIENT";
attr name="B.USERID",            title="Source user ID";
attr name="B.GROUPID",           title="Source group ID";
attr name="B.USERNAME",          title="Source user name";
attr name="B.GROUPNAME",         title="Source group name";
attr name="E.JP1_SOURCEHOST",    title="Event source host name";
attr name="B.SOURCESERVER",      title="Event-issuing server name";
attr name="B.SOURCEIPADDR",      title="Source IP address";
attr name="B.SOURCESEQNO",       title="Source serial number";
attr name="E.SEVERITY",          title="Event level";
attr name="E.USER_NAME",         title="User name";
attr name="E.PRODUCT_NAME",      title="Product name";
attr name="E.OBJECT_TYPE",       title="Object type";
attr name="E.OBJECT_NAME",       title="Object name";
attr name="E.ROOT_OBJECT_TYPE",  title="Root object type";
attr name="E.ROOT_OBJECT_NAME",  title="Root object name";
attr name="E.OBJECT_ID",         title="Object ID";
attr name="E.OCCURRENCE",        title="Occurrence";
attr name="E.START_TIME",        title="Start time", type="elapsed_time/date_
format:CLIENT";
attr name="E.END_TIME",          title="End time",type="elapsed_time/date_for
mat:CLIENT";
```

```
attr name="E.RESULT_CODE",      title="Result code";
attr name="E.JP1_GENERATE_SOURCE_SEQNO", title="Relation Event serial number
";
attr name="E.JP1_GENERATE_NAME",         title="Correlation event generatio
n condition name";
attr name="E.@JP1IM_ORIGINAL_SEVERITY",  title="Original severity level";
attr name="E.JP1_IMSUPPRESS_ID",   title="Suppressed event ID";
attr name="E.JP1_IMSUPPRESS_NAME", title="Repeated event condition name";
attr name="E.JP1_TRAP_ID",      title="Monitoring ID";
attr name="E.JP1_TRAP_NAME",    title="Log file trap name";
attr name="E.@JP1IM_CHANGE_MESSAGE_NAME",    title="Display message change d
efinition";
attr name="E.JP1_IMCOMEXCLUDE_ID",   title="Common exclude conditions group
ID";
attr name="E.JP1_IMCOMEXCLUDE_NAME", title="Common exclude conditions group
name";
attr name="E.JP1_IMCOMEXCLUDE_TARGET", title="Common exclude conditions grou
p target-for-exclusion";
attr name="E.SUGGESTION_ID", title="Suggestion ID";
attr name="E.TREE_SID", title="SID of the tree";
@define-block-end;
```

Definition file for extended event attributes (extended file)

Format

```
[@encode character-encoding]
@file type="extended-attributes-definition", version="0300";
@define-block type="event-attr-def";
attr name="attribute-name", title="item-name";
...
@define-block-end;
```

File

`template_extend_attr_ja.conf` (Japanese extended file)

`template_extend_attr_ja.conf.model` (model file for the Japanese extended file)

`template_extend_attr_en.conf` (English extended file)

`template_extend_attr_en.conf.model` (model file for the English extended file)

`template_extend_attr_zh.conf` (Chinese extended file)

`template_extend_attr_zh.conf.model` (model file for the Chinese extended file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\attribute\extend`

For a logical host:

shared-folder`\JP1Cons\conf\console\attribute\extend`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/attribute/extend`

For a logical host:

shared-directory`/jp1cons/conf/console/attribute/extend`

Description

The definition file for extended event attributes (extended file) defines program-specific extended attributes to be displayed as item names on the screen of JP1/IM - View or the integrated operation viewer or output as item names in event reports.

Note that the definition file included with JP1/IM - Manager is prefixed with `template_`. Rename the file to `extend_attr_ja.conf` before you use it.

For details about a definition file for extended event attributes that is not an extended file, see *Definition file for extended event attributes* in *Chapter 2. Definition Files*.

Creation timing

The files are created when JP1/IM - Manager is installed.

When the definitions are applied

The definitions in the definition file for extended event attributes (extended file) take effect after either of the following occurs:

- JP1/IM - Manager is restarted.
- The command `jco_spmd_reload` is executed.

Note that you must restart JP1/IM - View or the integrated operation viewer if the definition is applied while JP1/IM - View or the integrated operation viewer are connected.

Information that is specified

The definition file for extended event attributes (extended file) defines program-specific extended attributes to be displayed as item names on the screen or output as item names in event reports. The extended files are JP1/IM - Manager definition files that are defined for each language used by JP1/IM - Manager.

If you use extended files for multiple languages in JP1/IM - Manager, the same attribute names must be specified in all the extended files. Because the attributes to be displayed in JP1/IM - View or the integrated operation viewer are uniquely determined for the entire system, it is not possible to display different attributes for different JP1/IM - Views or the integrated operation viewer in each language.

If there is a mismatch in the attribute names specified in the extended files, the warning message `KAVB5820-W` will be output when you check the extended files using the `jcoattrfcheck` command. In addition, attributes not specified in the extended files might appear in JP1/IM - View or the integrated operation viewer. For example, if the attribute `E.SYSTEM` is specified only in the English extended file, `E.SYSTEM` will also appear in the Japanese and Chinese JP1/IM - Views. In this case, the item name of `E.SYSTEM` displayed in the Japanese and Chinese JP1/IM - Views will be identical to the attribute name, namely `E.SYSTEM`.

JP1/IM provides the `jcoattrfcheck` command for checking the contents of a definition file for extended event attributes (extended file). For details about this command, see *jcoattrfcheck* in *Chapter 1. Commands*.

You can specify the statements and blocks described in the table below in a definition file for extended event attributes (extended file).

Table 2–32: Statements and blocks that can be specified in a definition file for extended event attributes (extended file)

Statement or block	Description
`@encode` statement	Specifies the character encoding used in the definition file
`@file` statement	Declares the definition file type and version
Definition block for extended event attributes	Defines the display of event attributes

Any statement or block that is not listed in the table above is ignored. If a definition file for extended event attributes (extended file) includes an invalid element, the invalid line is ignored while other valid lines work successfully. However, an error is issued if an invalid element is found in a statement that can be read from a definition file for extended event attributes (non-extended file) but cannot be read from a definition file for extended event attributes (extended file), for example, the `block` statement (`block lang="";`). For details about definition files for extended event attributes (non-extended files), see *Definition file for extended event attributes* in *Chapter 2. Definition Files*.

Information that is specified (specification of character encoding)

`@encode`

Specifies the character encoding that is to be used in the definition file for extended event attributes (extended file).

Item names will be expressed in characters that can be represented in the character encoding specified in the `@encode` statement. In addition, the definition file for extended event attributes (extended file) will be saved in the character encoding specified in the `@encode` statement.

In the following circumstances, item names displayed in JP1/IM - View or the integrated operation viewer might be garbled:

- If the item name uses characters that cannot be represented in the character encoding specified in the `@encode` statement
- If the character encoding specified in the `@encode` statement does not match the character encoding in which the file was saved

If no `@encode` statement exists or if there is an error in the specified character set name that follows the `@encode` statement, the character set is determined automatically. However, depending on the content of the definition file, the character encoding might not be determined correctly.

The following character encodings can be specified.

Table 2–33: Definition file character encodings that can be specified

No.	Character encoding of file	Can be specified?	
		OS other than Linux	Linux
1	C	Y	Y
2	EUCJIS	Y	N
3	SJIS	Y	Y#
4	UTF-8	Y	Y
5	GB18030	Y	Y

Legend:

Y: Can be specified

N: Cannot be specified

#

Can be specified only in SUSE Linux.

Note:

If you use UTF-8 as the encoding to save a definition file, save the file without attaching a BOM (byte order mark).

An error is output in the following cases:

- A character encoding other than C, EUCJIS, SJIS, UTF-8, or GB18030 is specified
- The definition file does not begin with `@encode`
- `@encode` is not followed by a character encoding value

Information that is specified (rules for generating in-file statements)

`@file` *statement*

Declares that this is a definition file for extended event attributes (extended file) and that the version of the definition specification format is 0300. This statement is required.

This statement must be on the first line of the file. If the statement is not specified on the first line, the integrity of operations cannot be guaranteed.

Syntax

```
@file type="extended-attributes-definition", version="0300";
```

Information that is specified (rules for generating blocks in the definition file for extended event attributes)

This subsection describes the blocks that can be specified in a definition file for extended event attributes (extended file). If an invalid statement is specified in a block, an error is output but only the statement with the error is ignored.

Definition block for extended event attributes

This block associates the event attribute name with its display item name. You can specify this block only once within the definition file. If you specify more than one definition block for extended event attributes, no error or warning is output, but the second and subsequent blocks are ignored.

Types of statements that can be specified

You can specify the following statements in this block:

`attr` statement

Information that is specified (rules for generating statements in a definition block for extended event attributes)

`attr` statement

Specifies the name of a program-specific extended attribute and the item name corresponding to that attribute, which is to be displayed on the screen or in event reports. You can specify this statement up to 100 times in a block. If you specify more than 100 `attr` statements, message `KAVB5803-W` will be output when you check the definition file with the `jcoattrfcheck` command.

Syntax

`attr name=`*attribute-name*`, title=`*item-name*`;`

`name=`*attribute-name*

Specifies the name of the extended attribute. The format is as follows:

`"E.`*extended-attribute-name*`"`

For the attribute name, you can specify a name with a maximum length of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_).

If you specify an extended attribute name that exceeds 32 bytes, message `KAVB5803-W` will be output when you check the definition file with the `jcoattrfcheck` command or execute the `jcoevtreport` command. In addition, message `KAVB5822-W` will be output when the definition file for extended event attributes (extended file) is loaded when JP1/IM - Manager starts or the `jco_spmd_reload` command is executed.

Only a program-specific extended attribute can be specified. However, you cannot specify attributes that overlap with the extended attributes specified in the standard definition file for extended event attributes (`default.conf`), such as the event source host name (`E.JP1_SOURCEHOST`) or the log file trap name (`E.JP1_TRAP_NAME`). If you specify extended attributes that overlap with the standard definition file for extended event attributes (`default.conf`), the item names specified in the standard file will be applied.

If you specify extended attributes that overlap with the standard definition file for extended event attributes (`default.conf`), message `KAVB5802-W`[#] will be output after the definition file for extended event attributes (extended file) is loaded when you execute the `jcoevtreport` or `jcoattrfcheck` command. The `jcoevtreport` command proceeds by ignoring overlapping attributes specified in the definition file for extended event attributes (extended file). In addition, message `KAVB5822-W` will be output after the definition file for extended event attributes (extended file) is loaded when you restart JP1/IM - Manager or execute the `jco_spmd_reload` command. JP1/IM - Manager proceeds by ignoring overlapping attributes specified in the definition file for extended event attributes (extended file).

If you specify a basic attribute (`B.`*attribute-name*) or an IM attribute (`E.@`*attribute-name*), or some other attribute that is not an extended attribute (`E.`*attribute-name*), message `KAVB5821-W`[#] will be output after the definition file for extended event attributes (extended file) is loaded when you execute the `jcoevtreport` or `jcoattrfcheck` command. In addition, message `KAVB5822-W` will be output after the definition file for extended event attributes (extended file) is loaded when you restart JP1/IM - Manager or execute the `jco_spmd_reload` command.

#: When the `jcoevtreport` command generates reports successfully or when the `jcoattrfcheck` command checks the definition file completely, the return value of the commands is `0` (normal end), regardless of whether message `KAVB5802-W` or `KAVB5821-W` was output.

If you use extended files for multiple languages in JP1/IM - Manager, all the attribute names specified in the definition files for extended event attributes (extended files) must match. Otherwise, message `KAVB5820-W` will be output after the definition file for extended event attributes (extended file) is loaded when you execute the `jcoevtreport` or `jcoattrfcheck` command. In addition, message `KAVB5822-W` will be output after the definition file for extended event attributes (extended file) is loaded when you restart JP1/IM - Manager or execute the `jco_spmd_reload` command.

`title=`*item-name*

Defines the item name of the program-specific extended attribute. *item-name* is expressed in characters that can be represented in the character encoding specified in the `@encode` statement. *item-name* might appear garbled in JP1/IM - View if it uses characters that cannot be represented in the character encoding specified in the `@encode` statement.

In addition, *item-name* might appear garbled in CSV files if it uses characters that cannot be represented in the character encoding of the report output by the `jcoevtreport` command.

Specify a character string that will serve as the program-specific extended attribute's item name for display on the screen and output in event reports. Half-width kana characters and the comma (`,`) cannot be used in this parameter. If half-width kana characters and the comma (`,`) are specified in the character string, they will not be output correctly.

The maximum length of *item-name* is 255 bytes. If you specify more than 255 bytes for *item-name*, message `KAVB5803-W` will be output when you check the definition file with the `jcoattrfcheck` command or execute the `jcoevtreport` command. In addition, message `KAVB5822-W` will be output after the definition file for extended event attributes (extended file) is loaded when you restart JP1/IM - Manager or execute the `jco_spmd_reload` command.

Note:

If you specify program-specific extended attributes in the definition file for extended event attributes (extended file) that overlap with the attributes in the standard definition file for extended event attributes (`default.conf`), the program-specific extended attribute item names specified in the standard definition file for extended event attributes (`default.conf`) will be displayed in the list of events in the Event Console window and will be output in the CSV header that is output with event reports.

Example definition

The following shows an example of a definition file for extended event attributes (extended file):

```
@encode UTF-8
@file type="extended-attributes-definition", version="0300";
@define-block type="event-attr-def";
attr name="E.SYSTEM",    title="System name";
attr name="E.ROLE",     title="Server role";
@define-block-end;
```

Common-exclusion-conditions extended definition file

Format

```
DESC_VERSION=file-version
# comment-line
def conditions-group-name
    [cmt comment]
    id conditions-group-ID
    [valid {true | false}]
    [ex-target Exclusion target]
    [date start-date-end-date]
    [rtime start-time-end-time]
    [week day-of-week]
    cnd
        event-condition
    end-cnd
end-def

def conditions-group-name-2
...
end-def
   :
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines the event conditions or the applicable period of the extended-mode common exclusion-conditions.

Use the language encoding that is used by JP1/IM - Manager to specify this file.

In the following cases, the backup file for the common-exclusion-conditions extended definition file is output as `common_exclude_filter_backup.conf`.

- An error is still found in a regular expression after the operation mode of common exclusion-conditions is switched from the basic mode to the extended mode by the `jcochcefmode` command.
- When the operation mode is changed from the extended mode to the basic mode.

For details about the `jcochcefmode` command and the backup file for the common-exclusion-conditions extended definition file, see *jcochcefmode* in *Chapter 1. Commands*.

Note that if the event acquisition filter (for compatibility) is used, common exclusion-conditions cannot be used. If the event acquisition filter (for compatibility) is used, use the `jcochafmode` command to switch to event acquisition filters. For details about the `jcochafmode` command, see *jcochafmode (UNIX only)* in *Chapter 1. Commands*.

The maximum size of the common-exclusion-conditions extended definition file is 15 megabytes in Shift JIS code.

Note that the maximum size is the total of the common-exclusion-conditions extended definition file and the additional common exclusion conditions. Therefore, if you write definitions so that the common-exclusion-conditions extended definition file is 15 megabytes in JIS code, you cannot add the additional common exclusion definition conditions.

When the definitions are applied

The definitions take effect when the `-ef` option of the `jcochfilter` command is specified. For details about the `jcochfilter` command, see *jcochfilter* in *Chapter 1. Commands*.

Information that is specified

`DESC_VERSION=`*file-version*

Indicates the version of the extended definition file for the common exclusion-conditions. `1` or `2` can be specified. If this parameter is omitted, `1` is assumed.

`#` *comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

`def` to `end-def` (definition block)

These are the start and end parameters of the definition for the extended-mode common exclusion-conditions. The block from `def` to `end-def` can be omitted. After `def`, specify the name of the extended-mode common exclusion-conditions group. If you specify "`def`△△△*conditions-group-name-1*△△△*conditions-group-name-2*△△△", "△△*conditions-group-name-1*△△△*conditions-group-name-2*△△△" will be the definition name (Δ indicates a space).

Specify *conditions-group-name* so that it is unique within the common-exclusion-conditions extended definition file. You can specify a character string of 1 to 50 bytes in Shift JIS. The characters you can specify are characters other than control characters (`0x00` to `0x1F`, `0x7F` to `0x9F`).

A maximum of 2,500 definition blocks can be written.

Note that the maximum number is the total of the number of definition blocks written in the common-exclusion-conditions extended definition file and the number of additional common exclusion condition groups. Therefore, if you write 2,500 definition blocks in the common-exclusion-conditions extended definition file, you cannot create an additional common exclusion condition group.

`cmt` *comment*

Provides an explanation of the extended-mode common exclusion-conditions. This parameter can be omitted. Specify a character string of 1 to 1,024 bytes in Shift JIS code for the comment. Specifiable characters are other than control characters (`0x00` to `0x1F`, `0x7F` to `0x9F`).

`id` *conditions-group-ID*

Specifies the conditions group ID of the extended-mode common exclusion-conditions. You can specify a value from 0 to the maximum number of definitions minus 1. This parameter cannot be omitted.

The IDs you can specify for the `id` parameter is from 0 to 2,499.

`valid {true | false}`

Specifies whether to enable the extended-mode common exclusion-conditions.

This parameter is not case sensitive. If this parameter is omitted, `true` is assumed.

`ex-target` *Exclusion target*

Specifies the target of the exclusion. Specify the character string `action` in the *exclusion-target* to exclude JP1 events that satisfy a common exclusion-condition from automated-action execution. The character string is not case sensitive. If this parameter is omitted, JP1 events that satisfy a common exclusion-condition are excluded from the target to be collected. Only one occurrence of this parameter is allowed for each definition block. Note that this parameter is available only when the version of the common exclusion-conditions extended definition file is 2.

`date` *start-date*–*end-date*

Specifies the period during which the extended-mode common exclusion-conditions apply. This parameter can be omitted. Specify this parameter in the following format:

`date`Δ*YYYYMMDD-YYYYMMDD*

Legend: Δ: A space

The specifiable period is from `1970/01/01` to `2099/12/31`.

If this parameter is omitted, the extended-mode common exclusion-conditions always apply.

If the start date is omitted, the extended-mode common exclusion-conditions apply from the time they are defined until the end date. To omit the start date, specify only the end date in the following format:

`dateΔ-YYYYMMDD`

Legend: Δ: A space

If the end date is omitted, the conditions apply continuously from the start date. To omit the end date, specify only the start date using one of the following formats:

`dateΔYYYYMMDD`

`dateΔYYYYMMDD-`

Legend: Δ: A space

For details about the applicable period, see *4.2.7 Common exclusion-conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`rtime` *start-time*–*end-time*

Specifies the time during which the extended-mode common exclusion-conditions apply. This parameter can be omitted. Specify this parameter in the following format:

`rtime`Δ*HHMM*–*HHMM*

Legend: Δ: A space

If this parameter is omitted, 9:00 is assumed as the start time, and the end time will be 24 hours after that time. The start time cannot be omitted. If the end time is omitted, the conditions apply for 24 hours from the start time.

To omit the end time, specify only the start time using one of the following formats:

`rtimeΔHHMM`

`rtimeΔHHMM-`

Legend: Δ: A space

The time you can specify for the start time and the end time is from 00:00 to 23:59.

If you specify an end time earlier than the start time, the end time is treated as the time of the following day. Alternatively, if the same time is specified for the start time and the end time, the end time is treated as the time of the following day.

The following table lists the omission patterns of the parameter end time.

Table 2–34: Omission patterns of the end time for the rtime parameter

No.	Omission pattern	Description
1	`rtime`Δ*start-time*	Applied within 24 hours from the start time
2	`rtime`Δ*start-time-*	

No.	Omission pattern	Description
3	`rtime`Δ*start-time-end-time*	Applied from the start date to the end date.

Legend:

Δ: Single-byte space

Specify the start time and the end time in the *HHMM* format. Specify the hour for *HH*, and the minute for *MM*.

The application period includes the start time but not the end time. For example, if you specify Monday, and set the start time to 21:00 and the end time to 03:00, the application period is from 21:00:00 on Monday through 02:59:59 on Tuesday (the following day).

For details about the applicable period, see *4.2.7 Common exclusion-conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`week` *day-of-week*

Specifies a day of the week on which the extended-mode common exclusion-conditions apply. This parameter can be omitted. To specify two or more days of the week, separate the days by a comma (`,`). Use the following format:

`weekΔ0,1,2,3,4,5,6`

Legend: Δ: A space

Days of the week correspond to the following numeric values:

- Sunday: `0`
- Monday: `1`
- Tuesday: `2`
- Wednesday: `3`
- Thursday: `4`
- Friday: `5`
- Saturday: `6`

If the day of the week is omitted, all days of the week are assumed.

For details about the applicable period, see *4.2.7 Common exclusion-conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`cnd` to `end-cnd` (event condition block)

These parameters mark the start and end of the block that specifies the event conditions of the extended-mode common exclusion-conditions. An event condition block must be specified in a definition block. It cannot be omitted. A tab or a space before or after the `cnd` and `end-cnd` parameters is ignored.

You cannot specify multiple event condition blocks for one definition block.

event-condition

Specifies the conditions for excluding JP1 events by means of the extended-mode common exclusion-conditions. You can specify from 0 to 256 event conditions for the event condition block. The event conditions are connected with the AND condition. The following shows how JP1 event conditions are specified:

*attribute-name*Δ*comparison-keyword*Δ*operand*

Legend: Δ: A space

Note that a line that contains only spaces and tabs is ignored, and processing continues.

attribute-name

Specifies the name of the attribute you want to compare. To specify a basic attribute, prefix the name with `B.`. To specify an extended attribute (common information) or an extended attribute (program-specific information), prefix the name with `E.`. The attribute name is case sensitive.

The following table lists and describes the combinations of attribute names and comparison keywords and the operands that can be specified.

Table 2–35: Combinations of attribute names and comparison keywords and the operands that can be specified

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	`B.ID`	• `Match` • `Do not match`	Specifies the event ID of a JP1 event. • A maximum of 100 event IDs can be specified. • Specify the event IDs in hexadecimal notation. • Event IDs are not case sensitive. • The permitted range is from `0` to `7FFFFFFF`.
2	Reason for registration	`B.REASON`	• `Match` • `Do not match`	Specifies the reason for registration of a JP1 event. • A maximum of 100 reasons can be specified. • The permitted range is from `-2,147,483,648` to `2,147,483,647`.
3	Source process ID	`B.PROCESSID`	• `Match` • `Do not match`	Specifies the source process ID of the JP1 event source application. • A maximum of 100 source process IDs can be specified. • The permitted range is from `-2,147,483,648` to `2,147,483,647`.
4	Registered time	`B.TIME`	• `Time range`	Specifies the time that a JP1 event was registered in the event database on the source host. • Specify the time of an environment in which JP1/IM - Manager is running. • Specify the start date and time and the end date and time of the range or the period. • Comparison is possible when *start-date-and-time-of-the range≤time≤end-date-and-time-of-the range* is true.
5	Arrived time	`B.ARRIVEDTIME`	• `Time range`	Specifies the time that the JP1 event was registered in the event database on the manager host. • Specify the time of an environment in which JP1/IM - Manager is running. • Specify the start date and time and the end date and time of the range or the period.
6	Source user ID	`B.USERID`	• `Match` • `Do not match`	Specifies the user ID of the JP1 event source process. • A maximum of 100 source user IDs can be specified.

No.	Item	Attribute name	Comparison keyword	Operand
				• The permitted range is from `-2,147,483,648` to `2,147,483,647`.
7	Source group ID	`B.GROUPID`	• `Match` • `Do not match`	Specifies the group ID of the JP1 event source process. • A maximum of 100 source group IDs can be specified. • The permitted range is from `-2,147,483,648` to `2,147,483,647`.
8	Source user name	`B.USERNAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the user name of the JP1 event source process. • A maximum of 100 source user names can be specified. However, if a regular expression is specified, only one source user name is allowed. • The source user name is case sensitive
9	Source group name	`B.GROUPNAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the group name of the JP1 event source process. • A maximum of 100 source group names can be specified. However, if a regular expression is specified, only one source group name is allowed. • The source group name is case sensitive.
10	Source IP address	`B.SOURCEIPADDR`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the IP address of the event-issuing server for a JP1 event. • A maximum of 100 source IP addresses can be specified. However, if a regular expression is specified, only one source IP address is allowed. • Specify four-digit values in hexadecimal for an IPv6 address as shown below by using `0` to `9` and `a` to `f`. `a` to `f` must be lowercase. Example: `0011:2233:4455:6677:8899:aabb:ccdd:eeff` Uppercase letters, an IPv4-mapped address, an IPv4 compatible address, and an abbreviated IPv6 address cannot be specified.
11	Event-issuing server name (source host)#	`B.SOURCESERVER`	• `First characters` • `Match` • `Do not match` • `Is contained`	Specifies the source host (event server name) of a JP1 event. • A maximum of 100 event-issuing server names can be specified. However, if a regular expression

No.	Item	Attribute name	Comparison keyword	Operand
			- `Is not contained` - `Regular expression`	is specified, only one event-issuing server name is allowed. - The event-issuing server name is case sensitive.
12	Message	`B.MESSAGE`	- `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Sets the message of a JP1 event. - A maximum of 100 messages can be specified. However, if a regular expression is specified, only one message can be specified. - The message is case sensitive.
13	Event level (if the severity changing function is enabled, specifies the event level before the change)	`E.SEVERITY`	- `defined` - `notdefined` - `Match`	Specifies whether an event level exists and the JP1 event type. - When the comparison keyword is `Match`, two or more of the following event levels can be specified: `Emergency`, `Alert`, `Critical`, `Error`", `Warning`, `Notice`, `Information`, and `Debug`.
14	User name	`E.USER_NAME`	- `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Specifies the name of the user who issued a JP1 event. - A maximum of 100 user names can be specified. However, if a regular expression is used, only one user name is allowed. - The user name is case sensitive.
15	Product name	`E.PRODUCT_NAME`	- `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Specifies the name of the program that issued a JP1 event. - A maximum of 100 product names can be specified. However, if a regular expression is used, only one product name is allowed. - The produce name is case sensitive.
16	Object type	`E.OBJECT_TYPE`	- `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Specifies the type of a JP1 event object. - A maximum of 100 object types can be specified. However, if a regular expression is used, only one object type is allowed. - The object type is case sensitive.
17	Object name	`E.OBJECT_NAME`	- `First characters`	Specifies the name of a JP1 event object.

No.	Item	Attribute name	Comparison keyword	Operand
			• `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	• A maximum of 100 object names can be specified. However, if a regular expression is used, only one object name is allowed. • The object name is case sensitive.
18	Root object type	`E.ROOT_OBJECT_TYPE`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the root object type of a JP1 event. • A maximum of 100 root object types can be specified. However, if a regular expression is used, only one root object type is allowed. • The root object type is case sensitive.
19	Root object name	`E.ROOT_OBJECT_NAME`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the root object name of a JP1 event. • A maximum of 100 root object names can be specified. However, if a regular expression is used, only one root object name is allowed. • The root object name is case sensitive.
20	Object ID	`E.OBJECT_ID`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the object type of a JP1 event. • A maximum of 100 object IDs can be specified. However, if a regular expression is used, only one object ID is allowed. • The object ID is case sensitive.
21	Occurrence	`E.OCCURRENCE`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the occurrence of a JP1 event. • A maximum of 100 occurrences can be specified. However, if a regular expression is used, only one occurrence is allowed. • The occurrence is case sensitive.
22	Start time	`E.START_TIME`	• `Time range` • `First characters` • `Match` • `Do not match` • `Is contained`	Specifies the time to start or restart execution of a JP1 event. • When the comparison keyword is `Time range`: - Specify the start date and time and the end date and time of the range or the period.

No.	Item	Attribute name	Comparison keyword	Operand
			- `Is not contained` - `Regular expression`	- Comparison is possible when *start-date-and-time-of-the range≤time≤end-date-and-time-of-the range* is true. - When the attribute to be compared is a decimal value, the attribute is compared as the total number of seconds. • When the comparison keyword is not `Time range`: - A maximum of 100 start times can be specified. However, if a regular expression is specified, only one start time name is allowed. - Compare using a comparison keyword for which an operand is specified as a character string.
23	End time	`E.END_TIME`	- `Time range` - `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Specifies the time for ending execution of a JP1 event. • When the comparison keyword is `Time range`: - Specify the start date and time and the end date and time of the range or the period. - Comparison is possible when *start-date-and-time-of-the range≤time≤end-date-and-time-of-the range* is true. - When the attribute to be compared is a decimal value, the attribute is compared as the total number of seconds. • When the comparison keyword is not `Time range`: - A maximum of 100 end times can be specified. However, if a regular expression is specified, only one end time is allowed. - Compare using a comparison keyword for which an operand is specified as a character string.
24	Return code	`E.RESULT_CODE`	- `First characters` - `Match` - `Do not match` - `Is contained` - `Is not contained` - `Regular expression`	Specifies the return code of a JP1 event. • A maximum of 100 return codes can be specified. However, if a regular expression is used, only one return code is allowed. • The return code is case sensitive.
25	Event source host name#	`E.JP1_SOURCEHOST`	- `First characters` - `Match` - `Do not match`	Specifies the host name of the event source host for a JP1 event. • A maximum of 100 event source host names can be specified. However, if a regular expression

No.	Item	Attribute name	Comparison keyword	Operand
			• `Is contained` • `Is not contained` • `Regular expression`	is specified, only one event source host name is allowed. • The event source host name is case sensitive.
26	Extended attribute	`E.`*xxxxxxx*	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	Specifies the attribute name of the extended attribute for a JP1 event. • For the attribute name, you can specify a name with a maximum length of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_). • A maximum of 100 extended attributes can be specified. However, if a regular expression is specified, only one extended attribute is allowed. • The extended attribute is case sensitive.

#

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is `Match` or `Do not match`, you can specify a business group name in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than `Match` and `Do not match` is selected, a business group name specified in a path format is treated as a host name.

If the `-ignorecasehost` option of the `jcoimdef` command is set to `ON`, and a comparison keyword other than `Regular expression` is selected, the character string is no longer case sensitive.

comparison-keyword

Specifies `BEGIN` (begins with), `IN` (matches), `NOTIN` (does not match), `SUBSTR` (includes), `NOTSUBSTR` (does not include), or `REGEX` (regular expression), `TRANGE` (time range), `DEFINED` (defined), or `NOTDEFINED` (not defined) as the comparison keyword. The comparison keyword is case sensitive.

To use the `TRANGE` (time range) comparison keyword, specify it as shown in the following table.

Table 2–36: Format for specifying TRANGE

Comparison method		Format	Specifiable range	Specification example
Specifying date and time		*start-date-and-time*Δ*end-date-and-time*	*start-date-and-time*≤ *attribute-value*≤*end-date-and-time*	When May 1, 2018, 00:00:00 to May 31, 2018, 23:59:59 is specified: `20180501000000 20180531235959`
Specifying a period	*xx* minutes ago	*base-time*Δ − *period* `(minutes) MIN`	*base-time* - *period* `(minutes)`≤*attribute-value*≤*base-time*	To specify the period from 330 minutes earlier than May 1, 2018, 00:00:00 to the base time: `20180501000000 -330MIN`
	xx minutes later	*base-time*Δ + *period* `(minutes) MIN`	*base-time*≤*attribute-value*≤*base-time* + *period* `(minutes)`	To specify the period from May 1, 2018,

Comparison method		Format	Specifiable range	Specification example
				00:00:00 to 330 minutes later than the base time: `20180501000000 +330MIN`
	xx hours ago	*base-time*Δ − *period* `(hours) HOUR`	*base-time* - *period* `(hours)`≤*attribute-value*≤*base-time*	To specify the period from 120 hours earlier than May 1, 2018, 00:00:00 to the base time: `20180501000000 -120HOUR`
	xx hours later	*base-time*Δ + *period* `(hours) HOUR`	*base-time*≤*attribute-value*≤*base-time* + *period* `(hours)`	To specify the period from May 1, 2018, 00:00:00 to 120 hours later than the base time: `20180501000000 +120HOUR`
	xx days ago	*base-time*Δ − *period* `(days) DAY`	*base-time* - *period* `(days)`≤*attribute-value*≤*base-time*	To specify the period from 180 days earlier than May 1, 2018, 00:00:00 to the base time: `20180501000000 -180DAY`
	xx days later	*base-time*Δ + *period* `(days) DAY`	*base-time*≤*attribute-value*≤*base-time* + *period* `(days)`	To specify the period from May 1, 2018, 00:00:00 to 180 days later than the base time: `20180501000000 +180DAY`

Legend:

Δ: A space

Specify the start date and time, the end date and time, and the base time in *YYYYMMDDhhmmss* format. The period (minutes, hours, and days) must be specified as a numeric value from 1 to 9,999. `MIN`, `HOUR`, and `DAY` are case sensitive.

An error results if you specify a period and the calculated date and time from the base time does not fall in an acceptable time range (from UTC 1970-01-01

00:00:00 to UTC 2099-12-31 23:59:59).

Operand

Specifies a character string as the value to be compared with the attribute value specified by the comparison keyword. The operand is case sensitive.

If you specify two or more operands, separate them by one or more consecutive spaces or tabs. The OR condition is applied to the specified operands. Note that if a regular expression is specified, only one operand is allowed.

If you want to specify a space, a tab, an end-of-line code (CR or LF), or % as part of an operand, use the format shown in the table below. Note also that during maximum value checking for the definition format, each of these values is treated as a single character.

There is no limit on the maximum length of the operand. However, for Shift-JIS, the maximum number of event conditions (attribute name, comparison keyword, and operand) in `cnd` to `end-cnd` (event condition block) is 65,536 bytes.

No.	Value to be specified	How to specify
1	Tab (0x09)	`%09`
2	Space (0x20)	`%20`
3	% (0x25)	`%25`
4	Linefeed LF (0x0a)	`%0a`
5	Linefeed CR (0x0d)	`%0d`

Note:

- Relationship between the values of `date`, `rtime`, and `week`

  When `date`, `rtime`, and `week` are set, the common exclusion-condition is enabled on every week day of `week` during a period of days specified in `date` from the start time to the end time specified in `rtime`.

  When the end time of `rtime` indicates a time on the next day, the common exclusion-condition remains enabled until the end time on the next day.

  For details about the applicable period, see *4.2.7 Common exclusion-conditions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Example definition

When the following conditions exist, the example definition excludes events during the period from 2010/10/01 to 2010/10/31 on Mondays through Saturdays from 10:00 to 12:00:

- The event ID matches `1`.
- The event level is `Emergency` or `Alert`.
- The registered host is specified with a regular expression as follows:
  - `host[0-9][0-9]`

```
DESC_VERSION=1
# comment
def common-exclusion-conditions-group-1
    cmt expiration: 2010/10/31
    id 1
    valid true
    date 20101001-20101031
    week 1,2,3,4,5,6
    rtime 1000-1200
    cnd
        B.ID IN 00000001
        E.SEVERITY IN Emergency Alert
        B.SOURCESERVER REGEX host[0-9][0-9]
    end-cnd
end-def
```

The definition example below excludes events from automated-action execution from 23:00 to next day 02:00 on every Monday through Saturday during the period between April 1, 2017 and May 1, 2017 when the following conditions are true:

- The event ID is 2.
- The severity is `Emergency` or `Alert`.
- The source host matches the following regular expression:
  - `host[0-9][0-9]`

```
DESC_VERSION=2
# comment
def common-exclusion-conditions-group-1
    cmt expiration: 2017/05/01
    id 1
    valid true
    ex-target action
    date 20170401-20170501
    week 1,2,3,4,5,6
    rtime 2300-0200
    cnd
        B.ID IN 00000002
        E.SEVERITY IN Emergency Alert
        B.SOURCESERVER REGEX host[0-9][0-9]
    end-cnd
end-def
```

Common-exclusion-conditions display item definition file (common_exclude_filter_attr_list.conf)

Format

```
# comment-line
attribute-name
attribute-name
attribute-name
   .
   .
   .
attribute-name
```

File

`common_exclude_filter_attr_list.conf` (common-exclusion-conditions display item definition file)

`common_exclude_filter_attr_list.conf.model` (model file for the common-exclusion-conditions display item definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\filter\attr_list`

For a logical host:

shared-folder`\jp1cons\conf\console\filter\attr_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/filter/attr_list`

For a logical host:

shared-directory`/jp1cons/conf/console/filter/attr_list`

Description

This definition file specifies the items that are to be displayed in the **Attribute name** display area of the Common Exclusion-Conditions Settings (Extended) window. The display items specified in the common-exclusion-conditions display item definition file are displayed in the **Attribute name** display area of the Common Exclusion-Conditions Settings (Extended) window in the order they are specified.

When the definitions are applied

The definitions take effect when Central Console is started or when the definitions are reloaded by executing the `jco_spmd_reload` command.

Information that is specified

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

attribute-name

The items to be displayed in the **Attribute name** display area of the Common Exclusion-Conditions Settings (Extended) window are specified in the common-exclusion-conditions display item definition file. Write one attribute name corresponding to a display item on each line. A maximum of 0 to 256 display items can be specified.

The attribute name is case sensitive. Space and tab characters specified at the beginning or the end of the attribute name are ignored.

If you specify `SEPARATOR`, a horizontal line, such as `--------------------`, is displayed in the **Attribute name** display area of the Common Exclusion-Conditions Settings (Extended) window. You can use `SEPARATOR` to separate frequently used items from those used less frequently.

However, if you specify only `SEPARATOR`, only `--------------------` is displayed in the **Attribute name** display area. If you then select `--------------------`, you will be unable to set the attribute name.

The following table lists the specifiable attribute names.

Table 2–37: List of display items

No.	Display item	Attribute name
1	Event source host name#	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`
10	Message	`B.MESSAGE`
11	Product name	`E.PRODUCT_NAME`
12	Event ID	`B.ID`
13	Start time	`E.START_TIME`
14	End time	`E.END_TIME`
15	Registered time	`B.TIME`
16	Arrived time	`B.ARRIVEDTIME`
17	Extended attribute	`OTHER_EXTENDED_ATTRIBUTE`
18	Reason for registration	`B.REASON`
19	Source process ID	`B.PROCESSID`
20	Source user name	`B.USERNAME`
21	Source user ID	`B.USERID`
22	Source group name	`B.GROUPNAME`
23	Source group ID	`B.GROUPID`
24	Source IP address	`B.SOURCEIPADDR`
25	Object ID	`E.OBJECT_ID`

No.	Display item	Attribute name
26	Return code	E.RESULT_CODE
27	--------------------	SEPARATOR

Note:

If the same attribute name is specified twice, both specifications are ignored.

Also, if the common-exclusion-conditions display item definition file cannot be read, and the number of valid display items is 0, items 1 to 26 are displayed.

#

If the event source host mapping function is not enabled, the item is not displayed in the Common Exclusion Condition Settings (Extended) window.

Common-exclusion-conditions auto-input definition file (common_exclude_filter_auto_list.conf)

Format

```
# comment
[DEFAULT_NAME common-exclusion-conditions-group-name]
attribute-name
attribute-name
   .
   .
attribute-name
attribute-name
```

File

`common_exclude_filter_auto_list.conf`

`common_exclude_filter_auto_list.conf.model` (model file for the common-exclusion-conditions auto-input definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\filter\auto_list`

For a logical host:

shared-folder`\jp1cons\conf\console\filter\auto_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/filter/auto_list`

For a logical host:

shared-directory`/jp1cons/conf/console/filter/auto_list`

Description

This file defines the JP1 event attributes that are set automatically when the Common Exclusion-Conditions Settings (Extended) window opens. The window opens when a JP1 event is selected from the list of events in the Event Console window, and then **View** - **Exclude by Common Exclusion-Conditions** is chosen. You can also define a default name for the additional common exclusion conditions group.

When the definitions are applied

The definitions take effect when Central Console is started or when the definitions are re-read by executing the `jco_spmd_reload` command.

Information that is specified

`DEFAULT_NAME` *common-exclusion-conditions-group-name*

Specifies the identifier that defines the common exclusion conditions group name. The identifier must be on the first line in the file (the first line in the file that is not a null line or a comment line).

The common exclusion conditions group name specified for this parameter is displayed as the initial value when the Common Exclusion-Conditions Settings (Extended) window opens. The window opens when a JP1 event from the list of event in the Event Console window, and then **View - Exclude by Common Exclusion-Conditions** is chosen.

For the name, specify a character string with a maximum of 40 bytes. You can specify any character that is not a control character (`0x00` to `0x1F`, `0x7F` to `0x9F`). If a name with more than 40 bytes is specified, characters from the 41st are dropped, and the first 40 bytes of the character string are used as the common exclusion-conditions group name. If this parameter is omitted, `Add common exclusion conditions group` is assumed as the common exclusion-conditions group name.

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

attribute-name

For the common-exclusion-conditions auto-input definition file, specify the attribute of a JP1 event that is to be set as an event condition when the Common Exclusion-Conditions Settings (Extended) window opens. The Common Exclusion-Conditions Settings (Extended) window opens when a JP1 event from the list of JP1 events in the Event Console window is selected, and then **View - Exclude by Common Exclusion-Conditions** is chosen. The condition for the attribute name specified for this parameter is displayed as the initial value when the Common Exclusion-Conditions Settings (Extended) window opens. The window opens when a JP1 event from the list of JP1 events in the Event Console window is selected, and then **View - Exclude by Common Exclusion-Conditions** is chosen.

For the definition items, write on each line one attribute name of a JP1 event that will be set.

The attribute name is case sensitive. Any space or tab character at the beginning or at the end of the attribute name is ignored.

If the same attribute name is specified twice, it is ignored, and the `KAVB1160-W` message is output to the integrated trace log file.

The order of JP1 events to be displayed automatically in the **Event conditions** section of the Common Exclusion-Conditions Settings (Extended) window is determined by the order in which the attributes are written in the common-exclusion-conditions display item definition file (`common_exclude_filter_attr_list.conf`).

The following table lists the attribute names that can be specified.

Table 2–38: List of display items

No.	Display item	Attribute name
1	Event source host name	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`

No.	Display item	Attribute name
10	Message	B.MESSAGE
11	Product name	E.PRODUCT_NAME
12	Event ID	B.ID
13	Reason for registration	B.REASON
14	Source process ID	B.PROCESSID
15	Source user name	B.USERNAME
16	Source user ID	B.USERID
17	Source group name	B.GROUPNAME
18	Source group ID	B.GROUPID
19	Source IP address	B.SOURCEIPADDR
20	Object ID	E.OBJECT_ID
21	Return code	E.RESULT_CODE

Note:

If the same attribute name is specified twice, both specifications are ignored.

Also, if the common-exclusion-conditions auto-input definition file cannot be read, and the number of valid display items is 0, items 1 to 3 and items 10 to 12 are displayed.

Display item definition file for the repeated event condition (event_storm_attr_list.conf)

Format

```
# comment
attribute-name
attribute-name
   .
attribute-name
```

File

`event_storm_attr_list.conf` (Display item definition file for the repeated event condition)

`event_storm_attr_list.conf.model` (model file for the display item definition file for the repeated event condition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\event_storm\attr_list`

For a logical host:

shared-folder`\jp1cons\conf\console\event_storm\attr_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/event_storm/attr_list`

For a logical host:

shared-directory`/jp1cons/conf/console/event_storm/attr_list`

Description

Specifies the items to be displayed in the **Attribute name** display area of the Repeated Event Condition Settings window. The items are displayed in this area in the order in which they are specified in the file.

When the definitions are applied

The contents of the definition file take effect when Central Console is started and when the definitions are read again by executing the `jco_spmd_reload` command.

Information that is specified

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

attribute-name

In the display item definition file for the repeated event condition, specify an item to be displayed in the **Attribute name** display area of the Repeated Event Condition Settings window. Specify the attribute names of the items you want to be displayed by specifying one item per line. You can specify from 0 to 256 items.

An attribute name is case sensitive. Any space or tab characters immediately preceding or following the attribute name will be ignored.

If you specify SEPARATOR, a horizontal line like -------------------- is displayed in the **Attribute name** display area of the Repeated Event Condition Settings window. You can use SEPARATOR to separate items used frequently from those used infrequently.

However, if you specify only SEPARATOR, only -------------------- is displayed in the **Attribute name** display area. If you then select --------------------, you will be unable to set the attribute name.

The following table lists the attribute names that can be specified.

Table 2–39: List of display items

No.	Display item	Attribute name
1	Event source host name[#]	E.JP1_SOURCEHOST
2	Registered host name	B.SOURCESERVER
3	Event level	E.SEVERITY
4	Object type	E.OBJECT_TYPE
5	Object name	E.OBJECT_NAME
6	Root object type	E.ROOT_OBJECT_TYPE
7	Root object name	E.ROOT_OBJECT_NAME
8	Occurrence	E.OCCURRENCE
9	User name	E.USER_NAME
10	Message	B.MESSAGE
11	Product name	E.PRODUCT_NAME
12	Event ID	B.ID
13	Start time	E.START_TIME
14	End time	E.END_TIME
15	Registered time	B.TIME
16	Arrived time	B.ARRIVEDTIME
17	Program-specific extended attribute	OTHER_EXTENDED_ATTRIBUTE
18	Reason for registration	B.REASON
19	Source process ID	B.PROCESSID
20	Source user name	B.USERNAME
21	Source user ID	B.USERID
22	Source group name	B.GROUPNAME
23	Source group ID	B.GROUPID
24	Source IP address	B.SOURCEIPADDR
25	Object ID	E.OBJECT_ID
26	Result code	E.RESULT_CODE
27	--------------------	SEPARATOR

Note:

If an attribute name is specified twice, both specifications are ignored.

Also, if the display item definition file for the repeated event condition cannot be read, and the number of valid display items is 0, items 1 to 26 are displayed.

#

If the user mapping function of the event source host is not enabled, this item is not displayed in the Repeated Event Condition Settings window.

Auto-input definition file for the repeated event condition (event_storm_auto_list.conf)

Format

```
# comment
[DEFAULT_NAME repeated-event-condition-name]
attribute-name
attribute-name
  .
  .
attribute-name
attribute-name
```

File

`event_storm_auto_list.conf`

`event_storm_auto_list.conf.model` (model file for the auto-input definition file for the repeated event condition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\event_storm\auto_list`

For a logical host:

shared-folder`\jp1cons\conf\console\event_storm\auto_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/event_storm/auto_list`

For a logical host:

shared-directory`/jp1cons/conf/console/event_storm/auto_list`

Description

This file defines the JP1 event attributes that are set automatically when the Repeated Event Condition Settings window opens. The window opens when the user selects a JP1 event from the list of events in the Event Console window and then chooses **Display** - **Suppress by Repeated Event Conditions**. You can also define a default name for the repeated event condition.

When the definitions are applied

The contents of the definition file take effect when Central Console is started and when the definitions are re-loaded by executing the `jco_spmd_reload` command.

Information that is specified

`DEFAULT_NAME` *repeated-event-condition-name*

Indicates the identifier that defines the repeated event condition name. The identifier must be on the first line in the file (more specifically, the first line in the file that is not a null line or a comment line).

The common exclusion conditions group name specified for this parameter is displayed as the initial value when the Repeated Event Condition Settings window opens. The window opens when the user selects a JP1 event from the list of events in the Event Console window and then chooses **Display - Suppress by Repeated Event Conditions**.

For the name, you can specify a character string that does not exceed 40 bytes. You can specify any character that is not a control character (`0x00` to `0x1F`, `0x7F` to `0x9F`). If a name with more than 40 bytes is specified, characters from the 41st are dropped, and the first 40 bytes of the character string are used as the repeated event condition name. If this parameter is omitted, *additional-repetition-event-condition* is assumed as the repeated event condition name.

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

attribute-name

In the auto-input definition file for the repeated event condition, specify a JP1 event attribute to be set as an event condition when the Repeated Event Condition Settings window opens. The window opens when the user selects a JP1 event from the list of events in the Event Console window, and then chooses **Display - Suppress by Repeated Event Conditions**. The condition of the attribute name specified for this parameter is displayed as the initial value when the Repeated Event Condition Settings window opens. The window opens when the user selects a JP1 event from the list of events in the Event Console window, and then chooses **Display - Suppress by Repeated Event Conditions**.

Specify the attribute names of items that are to be set as definition items by specifying one item per line.

An attribute name is case sensitive. Any space or tab characters immediately preceding or following the attribute name will be ignored.

If the same attribute is specified twice, both specifications are ignored, and the `KAVB1896-W` message is output to the integrated trace log file.

The order of JP1 events that are displayed automatically in the **Event conditions** section of the Repeated Event Condition Settings window is determined by the order in which the attribute names are written in the display item definition file for the repeated event condition (`event_storm_attr_list.conf`).

The following table lists the attribute names that can be specified.

Table 2–40: List of display items

No.	Display item	Attribute name
1	Event source host name	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`
10	Message	`B.MESSAGE`
11	Product name	`E.PRODUCT_NAME`

No.	Display item	Attribute name
12	Event ID	`B.ID`
13	Reason for registration	`B.REASON`
14	Source process ID	`B.PROCESSID`
15	Source user name	`B.USERNAME`
16	Source user ID	`B.USERID`
17	Source group name	`B.GROUPNAME`
18	Source group ID	`B.GROUPID`
19	Source IP address	`B.SOURCEIPADDR`
20	Object ID	`E.OBJECT_ID`
21	Result code	`E.RESULT_CODE`

Note:

If the same attribute name is specified twice, both specifications are ignored.

Also, if the auto-input definition file for the repeated event condition cannot be read, and the number of valid display items is 0, items 1 to 3 and items 10 to 12 are displayed.

Status event definition file (processupdate.conf)

Format

```
[PROCESSUPDATE]
PROCESS_UPDATE_EVENT_OPTION={true | false}
[End]
```

File

`processupdate.conf` (status event definition file)

`processupdate.conf.model` (model file for the status event definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\processupdate\`

For a logical host:

shared-folder`\jp1cons\conf\processupdate\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/processupdate/`

For a logical host:

shared-directory`/jp1cons/conf/processupdate/`

Description

This file defines whether a JP1 event is to be issued when the action status changes.

When the definitions are applied

The setting specified in the status event definition file takes effect at the following time:

- When JP1/IM - Manager starts

Information that is specified

`PROCESS_UPDATE_EVENT_OPTION={true | false}`

Specifies whether a JP1 event (event ID: `3F11`) is to be issued when the action status changes. The value is not case sensitive.

Specify `true` if a JP1 event is to be issued when the action status changes.

Specify `false` if a JP1 event is not to be issued when the action status changes. The default is `false`.

If this parameter is omitted or an invalid value is specified, `false` is assumed.

For details about JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

Note

- If you specify that a JP1 event is to be issued, one instance of the JP1 event with ID `3F11` will be issued for each JP1 event for which an action is taken. For example, if you select multiple JP1 events on the **Severe Events** page on the Event Console window and their action status changes, as many JP1 events with ID `3F11` will be issued as there are JP1 events whose action status has changed.

  You should not enable this function when the action status of a large number of JP1 events will be changed by processing in the batch mode.

Correlation event generation system profile (egs_system.conf)

Format

```
VERSION=1

START_OPTION={cold | warm}
```

File

`egs_system.conf` (correlation event generation system profile)

`egs_system.conf.model` (model file for the correlation event generation system profile)

Storage directory

In Windows

For a physical host:

Console-path`\conf\evgen\profile\`

For a logical host:

shared-folder`\jp1cons\conf\evgen\profile\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/evgen/profile/`

For a logical host:

shared-directory`/jp1cons/conf/evgen/profile/`

Description

This file defines the start and stop operations for the Event Generation Service.

When the definitions are applied

The settings in the correlation event generation system profile take effect at the following times:

- When JP1/IM - Manager starts
- When the file is reloaded by the `jco_spmd_reload` command

Information that is specified

`VERSION=1`

Specifies the file version. There is no need to edit this parameter. If this parameter is omitted or a numeric value other than 1 is specified, `VERSION=1` is assumed.

`START_OPTION={cold | warm}`

Specifies the startup option for the Event Generation Service.

Specify the value that corresponds to the operation to be performed during start and stop processing. The permitted values are `cold` and `warm`. The default is `warm`. This value is not case sensitive. If the parameter is omitted or an invalid value is specified, `warm` is assumed.

The operations are different depending on whether or not the integrated monitoring database is used.

The table below describes the operation of the Event Generation Service during start and stop processing depending on whether `cold` or `warm` is specified when the integrated monitoring database is not used. Change the value as appropriate to your operations.

Table 2–41: Operation of the Event Generation Service during start and stop processing depending on the start option (when the integrated monitoring database is not used)

Start option	Operation of Event Generation Service	
	Operation during startup processing[#1]	Operation during stop processing
`cold`	When the start option was set to `cold` during the previous stop processing: JP1 events registered after the Event Generation Service started are subject to generation processing.	All correlation events under generation processing fail and are output to the correlation event generation history file.
	When the start option was set to `warm` during the previous stop processing: All correlation events under generation processing fail and the JP1 events acquired since the Event Generation Service started are subject to generation processing.	
`warm`	When the start option was set to `cold` during the previous stop processing: JP1 events are subject to generation processing beginning with the one that immediately follows the last JP1 event acquired by the Event Generation Service during the previous stop processing.	Information about the last JP1 event acquired before the service stopped, details of the generation processing, and the correlation event generation definition information are output to internal logs and saved.
	When the start option was set to `warm` during the previous stop processing: The correlation event generation processing performed during the previous stop processing is inherited, and JP1 events are subject to generation processing beginning with the one that immediately follows the last JP1 event acquired by the Event Generation Service during the previous stop processing.[#2]	

#1

When the Event Generation Service starts for the first time, it functions as follows, regardless of the start option value:

- The Event Generation Service acquires JP1 events that are registered after the Event Generation Service starts.
- The Event Generation Service loads the correlation event generation definition and starts processing according to the definition.

Note that the default is that correlation events are not generated because the correlation event generation definition has not been set.

#2

If the correlation event generation definition used when JP1/IM - Manager stopped differs from the definition used the next time JP1/IM - Manager starts, all correlation events under generation processing fail. After the contents are cleared, JP1 events are subject to generation processing again starting with the one that immediately follows the JP1 event acquired during the previous stop processing.

When the integrated monitoring database is used, the correlation event generation function associates the correlation event generation definition with the event acquired by the Event Base Service and then generates the correlation event.

It is possible to choose the position at which the Event Base Service is to start acquiring JP1 events from the JP1/Base event database after startup. Use the `-b` option to the `jcoimdef` command to choose where to start JP1 event acquisition.

The correlation event generation processing varies depending on the combination of the start option and the JP1 event acquisition start position, as shown in the following table.

Table 2–42: Operation of the Event Generation Service during start and stop processing depending on the start option (when the integrated monitoring database is used)

Start option	Value of -b option	Processing
`warm`	`-1` (default value)	The status of the JP1 events under correlation event generation processing is inherited. JP1 event acquisition starts from the next JP1 event after the last JP1 event acquired when the service stopped. If there is no such JP1 event, acquisition starts from the oldest JP1 event among the events registered in the event database.
	`0` to `144`	Message `KAJV2316-W` is output, and the status of the JP1 events under correlation event generation processing is not inherited.
`cold`	`-1` to `144`	All correlation event generation processing stops and the service terminates. The status of the JP1 events under correlation event generation processing is not inherited.

Note that when the integrated monitoring database is used, JP1 events that were once subject to correlation event generation processing are not subject to correlation event generation processing again.

If you run JP1/IM - Manager in a cluster system, change the setting to `warm`.

In the event of failover, products are stopped and started in the following order: stopping JP1/IM - Manager → stopping JP1/Base → starting JP1/Base → starting JP1/IM - Manager. If failover occurs while the parameter is set to `cold`, the system cannot acquire JP1 events that occur during the period of stopping JP1/IM - Manager → stopping JP1/Base and during the period of starting JP1/Base → starting JP1/IM - Manager. Therefore, if you leave the parameter set to `cold`, some JP1 events that are subject to generation processing might be missed.

Correlation event generation definition file

Format

```
VERSION={1 | 2}

#comment-line
[generation-condition-name]
TARGET=filtering-condition-for-the-correlation-target-range
CON=event-condition
TIMEOUT=timeout-period
TYPE=event-correlation-type
SAME_ATTRIBUTE=duplicate-attribute-value-condition
CORRELATION_NUM=maximum-correlation-number
SUCCESS_EVENT=correlation-approval-event
FAIL_EVENT=correlation-failure-event

[generation-condition-name]
TARGET=filtering-condition-for-the-correlation-target-range
CON=event-condition
TIMEOUT=timeout-period
TYPE=event-correlation-type
SAME_ATTRIBUTE=duplicate-attribute-value-condition
CORRELATION_NUM=maximum-correlation-number
SUCCESS_EVENT=correlation-approval-event
FAIL_EVENT=correlation-failure-event
          :
```

File

Use any file. However, the following limitations apply:

- The extension must be `.conf`.
- The file name can consist of only alphanumeric characters and the underscore (_).

Storage directory

In Windows

  Any folder

In UNIX

  Any directory

Description

This file defines JP1 event conditions that result in generation of correlation events and the correlation events that are generated when the JP1 event conditions are satisfied. Use the language encoding that is used by JP1/IM - Manager to specify this file.

When the definitions are applied

The definitions take effect after the correlation event generation definitions are applied by the `jcoegschange` command.

Information that is specified

VERSION={1 | 2}

Specifies the version of the correlation event generation definition file.

Specify either 1 or 2.

If you specify 1, none of the parameters listed below can be specified. To specify all the parameters described here, specify 2 in the VERSION parameter.

Table 2–43: Parameters that cannot be specified

Version	Parameter
1	TARGET
	SAME_ATTRIBUTE
	CORRELATION_NUM
2	None

Any zeros that are specified preceding the value are ignored. For example, VERSION=0001 is the same as VERSION=1. If this parameter is omitted, VERSION=1 is assumed.

If the specified value is neither 1 nor 2, a definition error results. Specifying VERSION more than once also results in a definition error.

#*comment-line*

A line beginning with a hash mark (#) is treated as a comment.

[*generation-condition-name*]

This is the start tag for a definition block that defines a correlation event generation condition. The information from the [*generation-condition-name*] tag to the information immediately before the next [*generation-condition-name*] tag constitutes one definition block. This tag cannot be omitted. You can define a maximum of 1,000 correlation event generation conditions. If more than 1,000 correlation event generation conditions are defined, a definition error occurs.

You must enclose the generation condition name in square brackets ([ ]). The generation condition name can consist of from 1 to 32 alphanumeric characters, the hyphen (-). underscore (_), and forward slash (/).

This name is case sensitive. For example, [JP1_HAKKOUZYOUKEN] is treated as being different from [jp1_hakkouzyouken].

Each generation condition name specified in the correlation event generation definition file must be unique. If the same generation condition name is specified more than once, the first name specified in the file is effective. A generation condition name cannot begin with IM_ (whether upper- or lowercase letters are used). If such a name is specified, a definition error occurs.

If you wish to specify a comment immediately following [*generation-condition-name*], use the format [*generation-condition-name*] #*comment-on-generation-condition*.

TARGET=*filtering-condition-for-the-correlation-target-range*

Specifies a filtering condition to narrow the range of JP1 events that are to be subject to generation of correlation events. If this parameter is omitted, all JP1 events that are acquired are subject to correlation event generation processing.

You can specify only one filtering condition for the correlation target range for each correlation event generation condition. If multiple filtering conditions are specified, a definition error results.

The following is the format:

- TARGET=*event-attribute-condition-1* [,*event-attribute-condition-2*...]

Separate multiple event attribute conditions with the comma (`,`). When multiple event attribute conditions are specified, it is assumed that they are connected with the AND condition, in which case the condition is satisfied only when a JP1 event that satisfies all the specified event attribute conditions is issued.

Specify an event attribute condition in the following format:

attribute-name comparison-condition attribute-value

The following table lists and describes the items that can be set for an event attribute condition.

Table 2–44: Items to be set for an event attribute condition

No.	Item	Description
1	*attribute-name*	Specifies a JP1 event basic or extended attribute. Prefix a basic attribute with `B.` and an extended attribute with `E.`. For example, to specify a message, specify `B.MESSAGE`. If you specify an extended attribute, express the character string that follows `E.` using from 1 to 32 bytes of characters. The following rules apply: • The character string must begin with an uppercase letter. • The character string beginning with byte 2 must be expressed using uppercase alphanumeric characters and the underscore (_). For details about the specifiable attribute names, see *Table 2-45 List of attribute names that can be specified in the filtering condition for the correlation target range*.
2	*comparison-condition*	Specifies a comparison condition. The supported comparison conditions and their meanings are listed below. If any other comparison condition is used, a definition error results. • `==`: `Match` • `!=`: `Does not match` • `^=`: `First characters` • `>=`: `Is contained` • `<=`: `Is not contained` • `*=`: `Regular expression` Note: For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
3	*attribute-value*	Specifies the value to be compared. You can specify a character string with a maximum of 2,048 bytes (1,023 bytes for JP1/IM - Manager version 09-10 or earlier) for an attribute value. If the value exceeds 2,048 bytes (1,023 bytes for JP1/IM - Manager version 09-10 or earlier), the definition is not valid. When specifying multiple event attribute conditions, you can specify a maximum of 2,305 bytes (1,280 bytes for JP1/IM - Manager version 09-10 or earlier) for the total of the attribute values for all conditions. If the value exceeds 2,305 bytes (1,280 bytes for JP1/IM - Manager version 09-10 or earlier), the definition is not valid. For example, if five event attribute conditions are specified, the total of these attributes must be equal to or smaller than 2,305 bytes (1,280 bytes for JP1/IM - Manager version 09-10 or earlier). Separate multiple attribute values with the semicolon (`;`). Any number of consecutive semicolons between attribute values is treated as a single semicolon (`;`). For example, `B.ID==A;;;;;B` is treated as `B.ID==A;B`. Example: If `E.`*xxx*`==A;B` is specified, the condition is satisfied when `E.`*xxx* matches `A` or `B`. To use a comma (,) or semicolon (;) as an attribute value, or use a space on each end of an attribute value, enclose the part you want to use as an attribute value in double quotation marks ("). To specify a double-quotation mark (`"`) or a backslash sign (`\`) in an attribute value, prefix it with a backslash sign (`\`).

- If you specify multiple attribute values for a single attribute name, the condition is satisfied as shown in the following examples:

  Example 1: If `E.`*xxx*`==A;B` is specified, the condition is satisfied when `E.`*xxx* matches `A` or `B`.

Example 2: If `E.`*xxx*`!=A;B` is specified, the condition is satisfied when `E.`*xxx* matches neither `A` nor `B`.

Example 3: If `E.`*xxx*`^=A;B` is specified, the condition is satisfied when `E.`*xxx* begins with `A` or `B`.

Example 4: If `E.`*xxx*`>=A;B` is specified, the condition is satisfied when `E.`*xxx* contains either `A` or `B`.

Example 5: If `E.`*xxx*`<=A;B` is specified, the condition is satisfied when `E.`*xxx* contains neither `A` nor `B`.

Example 6: If `E.`*xxx*`*=A;B` is specified, the condition is satisfied when `E.`*xxx* matches the regular expression of either `A` or `B`.

- Be careful about specifying the same attribute name more than once in the same attribute condition. The following combinations result in a definition error:

  • A combination that never matches

  - The message (`B.MESSAGE`) begins with `KAVB` and does not include `KAVB`.

  • Redundant combinations

  - The message (`B.MESSAGE`) begins with `KAVB` and contains `KAVB`.

- The system ignores any space (space and ASCII codes from `0x01` to `0x1F`) between an attribute name, a comparison condition, and an attribute value, at both ends of an attribute value separated by a semicolon, and at both ends of an event attribute condition.

  Example: The message matches `KAJV`*xxxx*`-IΔExecuted` or `Error`.

  A space is ignored if it is specified at the location of Δ below:

  `ΔB.MESSAGEΔ==Δ"KAJV`*xxxx*`-IΔExecuted";ΔErrorΔ`

  The following specifications are the same as the above example:

  `B.MESSAGE==KAJV`*xxxx*`-IΔExecuted;Error`

  `B.MESSAGE=="KAJV`*xxxx*`-IΔExecuted";Error`

- If you specify the event ID (`B.ID`) as the attribute name, the comparison condition must be a complete match (==).

The following table lists the attribute names that can be specified in the filtering condition for the correlation target range.

Table 2–45: List of attribute names that can be specified in the filtering condition for the correlation target range

No.	Attribute name	Item
1	`B.SOURCESERVER`#1	Event-issuing server name
2	`B.DESTSERVER`#1	Target event server name
3	`B.MESSAGE`	Message
4	`B.ID`	Event ID
5	`B.REASON`	Reason for registration
6	`B.USERID`	Source user ID
7	`B.GROUPID`	Source group ID
8	`B.USERNAME`	Source user name
9	`B.GROUPNAME`	Source group name
10	`E.JP1_SOURCEHOST`#1	Event source host name
11	`E.`*xxxxxxx*#2	Extended attribute (common information, user-specific information)

#1

If the integrated monitoring database and the IM Configuration Management database are enabled, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, a business group name specified in a path format is treated as a host name.

If the `-ignorecasehost` option of the `jcoimdef` command is set to `ON`, and a comparison keyword other than `Regular expression` is selected, the character string is no longer case sensitive.

#2

You can also specify a JP1 product-specific extended attribute. For example, the program-specific extended attribute for the JP1/AJS job execution host is `E.C0`. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

`CON=`*event-condition*

Defines the targets of correlation event generation processing or a condition for JP1 events that are to be excluded as targets. You can specify multiple event conditions. There must be at least one definition in each correlation event generation condition. You can define a maximum of 10 event conditions. If no event condition is defined or the specified definition is invalid, a definition error results.

The following is the specification format:

`CON={NOT|[CID:`*n*`]},`*event-attribute-condition-1* `[,` *event-attribute-condition-2*`[,` *event-attribute-condition-3* `...] ]`

If you specify multiple event attribute conditions, separate them with the comma (`,`). When multiple event attribute conditions are specified, they are assumed to be connected with the AND condition, in which case the condition is satisfied only when a JP1 event that satisfies all the specified event attribute conditions is issued.

The following table lists and describes the items to be set for the event condition.

Table 2–46: Items to be set for the event condition

No.	Item	Description
1	`NOT`	Specifies that JP1 events are to be excluded as targets of correlation event generation processing. When you specify `NOT` as an event condition, that condition is applied first, regardless of the sequence in which the event conditions (`CON` statements) are defined.
2	`CID:`*n*	Specifies an ID for the condition. Specify this item to use a variable to pass the correlation source event information to another parameter (`SAME_ATTRIBUTE`, `SUCCESS_EVENT`). The permitted values are the integers in the range from 1 to 999. For example, if the correlation source event consists of multiple JP1 events and the `$EV`*n*`_B.MESSAGE` variable is specified in the `SUCCESS_EVENT` parameter, message information for the correlation source event can be passed to the correlation event. If this parameter is omitted, information cannot be passed to another parameter. If the specified value is preceded by zeros or the same `CID` is specified more than once, a definition error results.
3	*event -attribute-condition*	Specifies the event attribute condition in the following format: Format: *attribute-name comparison-condition attribute-value* *attribute-name* Specifies a JP1 event basic or extended attribute. Prefix a basic attribute with `B.` and an extended attribute with `E.`. For example, to specify the message, specify `B.MESSAGE`. If you specify an extended attribute, express the character string that follows `E.` using from 1 to 32 bytes of characters. The following rules apply: The character string must begin with an uppercase letter. The character string beginning in byte 2 must be expressed using uppercase alphanumeric characters and the underscore (_).

No.	Item	Description
		For details about basic and extended attributes, see *3.1 Attributes of JP1 events*. To specify a product-specific extended attribute, consult the documentation for that product. If you specify product-specific extended attributes, consult the documentation for the products that issue the JP1 events. Note that you cannot specify the source IP address (SOURCEIPADDR). *comparison-condition* and *attribute value* The rules for specifying the comparison condition and attribute value are the same as for specifying the event attribute condition in TARGET. See *Table 2-44 Items to be set for an event attribute condition* and the information following the table.

TIMEOUT=*timeout-period*

Specifies the timeout period for the correlation event generation condition. The permitted value range is from 1 to 86,400 (seconds). If this parameter is omitted, 60 seconds is assumed.

TYPE=*event-correlation-type*

Specifies the event correlation type.

The three event correlation types that can be specified are sequence, combination, and threshold, which are explained below:

- sequence

  The correlation event generation condition is satisfied if the JP1 events that satisfy the defined event condition are issued in the order defined.

- combination

  The correlation event generation condition is satisfied if a JP1 event that satisfies the combination of defined event conditions is issued regardless of the sequence.

- threshold:*n*

  The correlation event generation condition is satisfied if the number of JP1 events that satisfy the defined event condition reaches the threshold. If multiple event conditions are defined, the correlation event generation condition is satisfied if the total number of JP1 events that satisfy any of the defined conditions reaches the threshold.

  The value permitted for the threshold is from 1 to 100 (count). For example, if the threshold is 10, specify as follows:

  threshold:10

This parameter is not case sensitive. If the event correlation type is omitted, combination is assumed.

SAME_ATTRIBUTE=*duplicate-attribute-value-condition*

Specifies the duplicate attribute value condition.

Define this parameter to group the JP1 events (correlation source events) that satisfy the event condition for an attribute value and to generate a correlation event for the group.

You can define a maximum of 3 duplicate attribute value conditions per correlation event generation condition. This parameter is optional.

The following shows the format:

- SAME_ATTRIBUTE=*attribute-name* | {$EV*n*_*attribute-name* | $EV*n*_ENV*o*} [, {$EV*n*_*attribute-name* | $EV*n*_ENV*o*} ...]

The following table lists and describes the items to be set for the duplicate attribute value condition.

Table 2–47: Items to be set for the duplicate attribute value condition

No.	Item	Description
1	*attribute-name*	Specifies a JP1 event basic or extended attribute. The attribute value of the correlation source event that corresponds to the attribute name specified here becomes the grouping key. You can specify only one *attribute-name* per *duplicate-attribute-value-condition*. Prefix a basic attribute with `B.` and an extended attribute with `E.` If you specify an extended attribute, express the character string that follows `E.` using from 1 to 32 bytes of characters. The following rules apply: • The character string must begin with an uppercase letter. • The character string beginning in byte 2 must be expressed as uppercase alphanumeric characters and the underscore (_). For details about the specifiable attribute names, see *Table 2-48 List of attribute names that can be specified in the duplicate attribute value condition*.
2	Variable `$EV`*n*`_`*attribute-name*	Specify this parameter if the attribute value to be used as the grouping key belongs to an attribute that varies for each correlation source event. For example, specify this parameter to use attribute `A'` of correlation source event `A` and attribute `B'` of correlation source event `B` as the grouping key. You can specify a maximum total of 10 `$EV`*n*`_`*attribute-name* and `$EV`*n*`_ENV`*o* parameters per duplicate attribute value condition. For details, see *(1)(a) Using an attribute value of the correlation source event as the duplicate attribute value condition*.
3	Variable `$EV`*n*`_ENV`*o*	Specify this parameter to use part of the attribute value of a correlation source event as the duplicate attribute value condition. For example, specify this parameter to use part of the message (`B.MESSAGE`) as the grouping key. You can specify a maximum total of 10 `$EV`*n*`_ENV`*o* and `$EV`*n*`_`*attribute-name* parameters per duplicate attribute value condition. For details, see *(1)(b) Using part of an attribute value of the correlation source event as the duplicate attribute value condition*.

- The attribute name and the value that is replaced with a variable (an attribute value or part of an attribute value) are case sensitive. Only values that perfect matches are able to be a duplicate attribute value condition.
- If the attribute name and the value that is replaced with a variable (attribute value or part of an attribute value) are not in the correlation source event, they are replaced with the null character (0 byte). This means that the null character is used as the grouping key. If this occurs, the following character string is output to the correlation event generation history file:

  `A JP1 event that matches the correlation event generation condition occurred and correlation event generation processing started, but the event attribute defined in that attribute value condition was not found in the JP1 event. (`*generation-condition-name*`(`*generation-processing-number*`)` *serial-number attribute-name*`)`

- If you specify `SAME_ATTRIBUTE=`*duplicate-attribute-value-condition* more than once, a correlation event is generated for each duplicate attribute value condition.

  For example, to issue a correlation event for each host name (`B.SOURCESERVER`) and user name (`B.USERNAME`), define as follows:

```
:
SAME_ATTRIBUTE=B.SOURCESERVER
SAME_ATTRIBUTE=B.USERNAME
:
```

- If you specify multiple variables in the duplicate attribute value condition, separate them with the comma (`,`). A correlation event is generated for each attribute value that is replaced with a variable.
- The system ignores any space (space and ASCII codes from `0x01` to `0x1F`) between an attribute name and a variable (`$EV`*n*`_`*attribute-name*, `$EV`*n*`_ENV`*o*) and at both ends of a duplicate attribute value condition (Δ in the following example):

  Example:

  `ΔSAME_ATTRIBUTEΔ=Δ$EV1_ENV1Δ,Δ$EV2_ENV2Δ`

The following table lists the attribute names that can be specified in the duplicate attribute value condition

Table 2–48: List of attribute names that can be specified in the duplicate attribute value condition

No.	Attribute name	Item
1	`B.SOURCESERVER`	Event-issuing server name
2	`B.DESTSERVER`	Target event server name
3	`B.MESSAGE`	Message
4	`B.ID`	Event ID
5	`B.REASON`	Reason for registration
6	`B.USERID`	Source user ID
7	`B.GROUPID`	Source group ID
8	`B.USERNAME`	Source user name
9	`B.GROUPNAME`	Source group name
10	`E.`*xxxxxxx*#	Extended attribute (common information, user-specific information)

#

You can also specify a JP1 product-specific extended attribute. For example, the product-specific extended attribute for the JP1/AJS job execution host is `E.C0`. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

`CORRELATION_NUM=`*maximum-correlation-number*

Specifies the maximum number of JP1 event sets that can be held by the correlation event generation condition. Only one maximum correlation number can be defined for a single correlation event generation condition.

The permitted value range is from 1 to 1,024 (sets). If this parameter is omitted, 10 sets is assumed.

Note:

It is not recommended to specify `CORRELATION_NUM` for many correlation event generation conditions and a large value for the maximum correlation number.

Doing so will increase the number of JP1 event sets that need to be processed concurrently by the Event Generation Service, and result in an increase in the amount of memory required and a reduction in processing speed.

The maximum number of JP1 event sets that can be issued concurrently by all correlation event generation conditions is 20,000 sets. When 20,000 sets have been issued concurrently, a JP1 event (event ID: `00003F28`) is output; until the number of sets drops below 20,000, no more processing is performed even if new JP1 events that satisfy the event conditions are issued.

`SUCCESS_EVENT=`*correlation-approval-event*

Defines the JP1 event (correlation event) that is to be issued when the correlation event generation condition results in correlation approval. Only one correlation approval event can be defined for a correlation event generation condition.

For details about the conditions that result in correlation approval, see *4.3.6(1) Generation condition satisfied* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you have defined `FAIL_EVENT=`*correlation-failure-event* in the correlation event generation condition, you can omit this parameter. When this parameter is omitted, no correlation approval event is issued, even when the correlation event generation condition results in correlation approval.

Specify the correlation approval event in the following format:

attribute-name`:`*attribute-value*

The following describes each item.

attribute-name

Specifies a JP1 event basic or extended attribute (correlation source event). Prefix a basic attribute with `B.` and an extended attribute with `E.` If you specify an extended attribute, express the character string that follows `E.` using from 1 to 32 bytes of characters. The following rules apply:

- The character string must begin with an uppercase letter.
- The character string beginning in byte 2 must be expressed as uppercase alphanumeric characters and the underscore (_).

You can specify any value for the following attributes:

- Event ID (`B.ID`)
- Message (`B.MESSAGE`)
- Extended attributes, except for those listed in the table below.

Table 2–49: Extended attributes for which a value cannot be specified

Attribute type	Item	Attribute name	Description
Common information	Product name	`E.PRODUCT_NAME`	`/HITACHI/JP1/IM/GENERATE_EVENT`
	Object type	`E.OBJECT_TYPE`	`SERVICE`
	Object name	`E.OBJECT_NAME`	`EGS`
	Occurrence	`E.OCCURRENCE`	`SUCCESS`
User-specific information	Relation Event serial number	`E.JP1_GENERATE_SOURCE_SEQNO`	Stores the serial numbers of the correlation source events separated by the space: *serial-number-1*Δ*serial-number-2*Δ*serial-number-3*. . .*serial-number-n* The maximum value of *n* is 100.
	Correlation event generation condition name	`E.JP1_GENERATE_NAME`	Name of correlation event generation condition that is satisfied
	Reserved word	Extended attribute beginning with `E.JP1_`	Extended attribute reserved by JP1/IM - Manager (other than the event source host name (`E.JP1_SOURCEHOST`))

If you want to pass the attribute value of a correlation source event to the correlation event, specify a variable. Specify *correlation-approval-event* in the following format:

attribute-name`:$EV`*n*`_`*attribute-name*

In this case, specify the correlation source event to be inherited by `CID` of the event condition and then specify the value of `CID` in *n*. Specify a variable to the right of the colon.

For details, see *(2)(a) Passing an attribute value of the correlation source event to an attribute value of the correlation event*.

If you want to specify a threshold (`threshold`) as the event correlation type and pass an attribute value of the correlation source event to the correlation event, specify *correlation-approval-event* in the following format:

attribute-name:$EV*n*_*m*_*attribute-name*

In this case, specify the correlation source event to be inherited by CID and then specify in *n* the value of CID. Specify a variable to the right of the colon. Also, specify in *m* the location of the correlation source event whose attribute value is to be passed.

For details, see *(2)(b) Passing an attribute value of the correlation source event to an attribute value of the correlation event (when the event correlation type is threshold)*.

If you wish to pass a portion of an attribute value of the correlation source event to the correlation event, specify the $EV*n*_ENV*o* variable. Use a regular expression to specify the event condition and enclose the portion of the attribute value to be acquired in parentheses.

Specify *correlation-approval-event* in the following format:

attribute-name:$EV*n*_ENV*o*

In this case, specify the correlation source event to be passed to CID and specify the value of CID in *n*. In *o* of ENV*o*, specify the acquisition order.

For details, see *(2)(c) Passing part of an attribute value of the correlation source event to the correlation event*.

For details about basic and extended attributes, see *3.1 Attributes of JP1 events*. If you specify product-specific extended attributes, consult the documentation for the products that issue JP1 events.

- You can specify multiple items in *correlation source event* by separating them with the comma (,).
- Make sure that you specify the event ID of a basic attribute (B.ID). The permitted range of event IDs is from 0 to 1FFF and from 7FFF8000 to 7FFFFFFF. If the event ID is not specified, 0 is set as the event ID.
- The maximum length of a single correlation approval event is 8,192 bytes. The maximum length of B.MESSAGE is 1,023 bytes. These maximum lengths include spaces but do not include linefeed codes.
- The system ignores any space (space and ASCII codes from 0x01 to 0x1F) between an attribute name and an attribute value and at both ends of SUCCESS_EVENT=*correlation-approval-event* (the space is represented by Δ in the following example).

  Example:

  ΔSUCCESS_EVENTΔ=ΔB.IDΔ:Δ1Δ
- To use a comma (,) or a space in an attribute value, enclose it in double-quotation marks (").
- To specify a double-quotation mark (") or a backslash (\), prefix it with a backslash (\) so that the value becomes \" or \\.

  To restore a special character (^ $. * + ? | ( ) { } [ ] \) to its original meaning, prefix it with two backslash signs so that the value becomes \\*special-character*.

  For example, to treat $ as a normal character, specify it as \\$. Also, to give \ its original meaning, specify \\\\.
- If you omit an attribute value, nothing is set when a correlation event is generated. If you omit the attribute value of an attribute name (B.ID), 0 is set.
- To specify a setting following the $EV*n*_*attribute-name* variable, specify a space (indicated by Δ in the example below) after the variable.

  Example:

  SUCCESS_EVENT=B.MESSAGE:"$EV*n*_B.IDΔ$EV*n*_B.TIMEΔ..."
- If you use a variable and there is no matching attribute name, the variable is replaced with a space. If the variable would be replaced when the correlation event is generated with an attribute value that exceeds the permitted maximum value, the correlation event is not generated.
- Up to 94 extended attributes can be specified.

FAIL_EVENT=*correlation-failure-event*

Defines a JP1 event (correlation event) that is to be issued when the correlation event generation condition results in a correlation failure. You can define only one correlation failure event per correlation event generation condition. For details about the conditions that result in a correlation failure, see *4.3.6(2) Generation condition fails* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you have specified SUCCESS_EVENT=*correlation-approval-event* in the correlation event generation conditions, you can omit this parameter. When this parameter is omitted, no correlation failure event is issued even if a correlation event generation condition results in a failure.

Specify *correlation-failure-event* in the same format as used for a correlation approval event. For details, see *SUCCESS_EVENT=correlation-approval-event*.

(1) Using a variable in the duplicate attribute value condition (SAME_ATTRIBUTE)

This subsection describes how to use a variable ($EV*n* or $EV*n*_ENV*o*) in the duplicate attribute value condition (SAME_ATTRIBUTE).

(a) Using an attribute value of the correlation source event as the duplicate attribute value condition

To use an attribute value of the correlation source event as the duplicate attribute value condition, use the $EV*n*_*attribute-name* variable. The format is as follows:

- SAME_ATTRIBUTE=$EV*n*_*attribute-name*

For *n*, specify the value that corresponds to the condition ID (CID) of the event condition. A value from 1 to 999 can be specified for the condition ID.

For *attribute-name*, specify the attribute name that is to be used as the grouping key. For details about the specifiable attributes names, see *Table 2-48 List of attribute names that can be specified in the duplicate attribute value condition*.

For example, the following definition associates JP1 events that have attribute values whose host information is different, such as a JP1 event of Windows log trapping (event ID: 00003A71) and a JP1 event issued by JP1/AJS (event ID: 00004107), and generates a correlation event for each host:

```
CON=CID:1,B.ID==3A71,E.A0==host1;host2
CON=CID:2,B.ID==4107,E.C0==host1;host2
           :
SAME_ATTRIBUTE=$EV1_E.A0,$EV2_E.C0
           :
```

(b) Using part of an attribute value of the correlation source event as the duplicate attribute value condition

To use part of the attribute value of a correlation source event as the duplicate attribute value condition, use the $EV*n*_ENV*o* variable. The format is as follows:

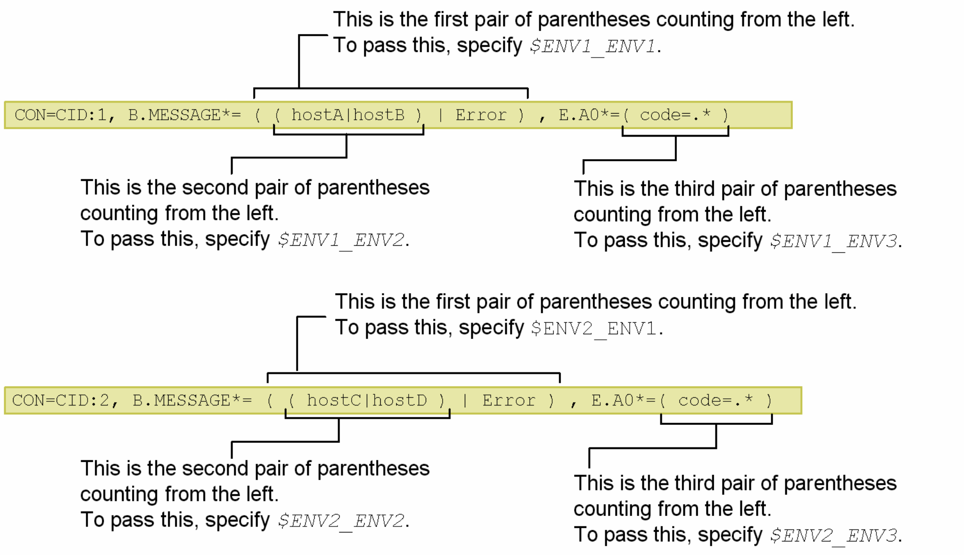
- SAME_ATTRIBUTE=$EV*n*_ENV*o*

When you specify $EV*n*_ENV*o*, use a regular expression (*=) to specify the event condition and enclose the part of the attribute value that is to be acquired in parentheses. For *n*, specify the value that corresponds to the condition ID (CID) of the event condition. A value from 1 to 999 can be specified for the condition ID.

In *o* of ENV*o*, specify the acquisition order. The acquisition order is based on the order of the parentheses in the right-hand term of the event condition, counting the pairs of parentheses from left to right. A value from 1 to 9 can be specified for the acquisition order.

The following figure shows the correspondence between the event condition (CON) and the part that is acquired by $EV*n*_ENV*o*.

Figure 2–3: Correspondence between the event condition (CON) and the part that is acquired by $EVn_ENVo


This is the first pair of parentheses counting from the left.
To pass this, specify $ENV1_ENV1.
CON=CID:1, B.MESSAGE*= ((hostA|hostB) | Error) , E.A0*=(code=.*)
This is the second pair of parentheses counting from the left.
To pass this, specify $ENV1_ENV2.
This is the third pair of parentheses counting from the left.
To pass this, specify $ENV1_ENV3.
This is the first pair of parentheses counting from the left.
To pass this, specify $ENV2_ENV1.
CON=CID:2, B.MESSAGE*= ((hostC|hostD) | Error) , E.A0*=(code=.*)
This is the second pair of parentheses counting from the left.
To pass this, specify $ENV2_ENV2.
This is the third pair of parentheses counting from the left.
To pass this, specify $ENV2_ENV3.

If there are multiple event attribute conditions that specify regular expressions in a single event condition (CON), count the pairs of parentheses from left to right and set in *o* the order of the pair enclosing the attribute value that is to be acquired.

For example, if you want to issue correlation events for each event that has the same host name in the message in the correlation source event, define as follows:

```
CON=CID:1, B.ID==1001, B.MESSAGE*=.*HOST=(.*\\))
TYPE=threshold:5
SAME_ATTRIBUTE=$EV1_ENV1
          :
```

(2) Using a variable in the correlation approval event (SUCCESS_EVENT)

To pass an attribute value of the correlation source event to the correlation event, use a variable in the correlation approval event (SUCCESS_EVENT).

(a) Passing an attribute value of the correlation source event to an attribute value of the correlation event

To pass an attribute value of the correlation source event to an attribute value of the correlation event, use the $EV*n*_*attribute-name* variable. The format is as follows:

- SUCCESS_EVENT=*attribute-name*:$EV*n*_*attribute-name*

For *n*, specify the condition ID (CID) that was specified in the event condition. For the right-hand *attribute-name*, specify the attribute that is to be passed from the correlation source event. Note that if the event ID (B.ID) is specified in the left-hand *attribute-name*, an attribute value of the correlation source event cannot be passed.

The following table lists the attribute names that can be specified in the variable.

Table 2–50: List of attribute names that can be specified in the variable

No.	Attribute name	Item	Format
1	B.SEQNO	Serial number	Numeric value
2	B.ID	Event ID	*basic-part*:*extended-part* in hexadecimal notation
3	B.PROCESSID	Source process ID	Numeric value

No.	Attribute name	Item	Format
4	`B.TIME`	Registered time	*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*#1
5	`B.ARRIVEDTIME`	Arrived time	*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*#1
6	`B.REASON`	Reason for registration	Character string
7	`B.USERID`	Source user ID	Numeric value
8	`B.GROUPID`	Source group ID	Numeric value
9	`B.USERNAME`	Source user name	Character string
10	`B.GROUPNAME`	Source group name	Character string
11	`B.SOURCESERVER`	Event-issuing server name	Character string
12	`B.DESTSERVER`	Target event server name	Character string
13	`B.SOURCESEQNO`	Source serial number	Numeric value
14	`B.MESSAGE`	Message	Character string
15	`E.SEVERITY`	Event level	Character string
16	`E.USER_NAME`	User name	Character string
17	`E.PRODUCT_NAME`	Product name	Character string
18	`E.OBJECT_TYPE`	Object type	Character string
19	`E.OBJECT_NAME`	Object name	Character string
20	`E.ROOT_OBJECT_TYPE`	Root object type	Character string
21	`E.ROOT_OBJECT_NAME`	Root object name	Character string
22	`E.OBJECT_ID`	Object ID	Character string
23	`E.OCCURRENCE`	Occurrence	Character string
24	`E.START_TIME`	Start time	*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*#1
25	`E.END_TIME`	End time	*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*#1
26	`E.`*xxxxxx*#2	Other extended attribute	Character string

#1

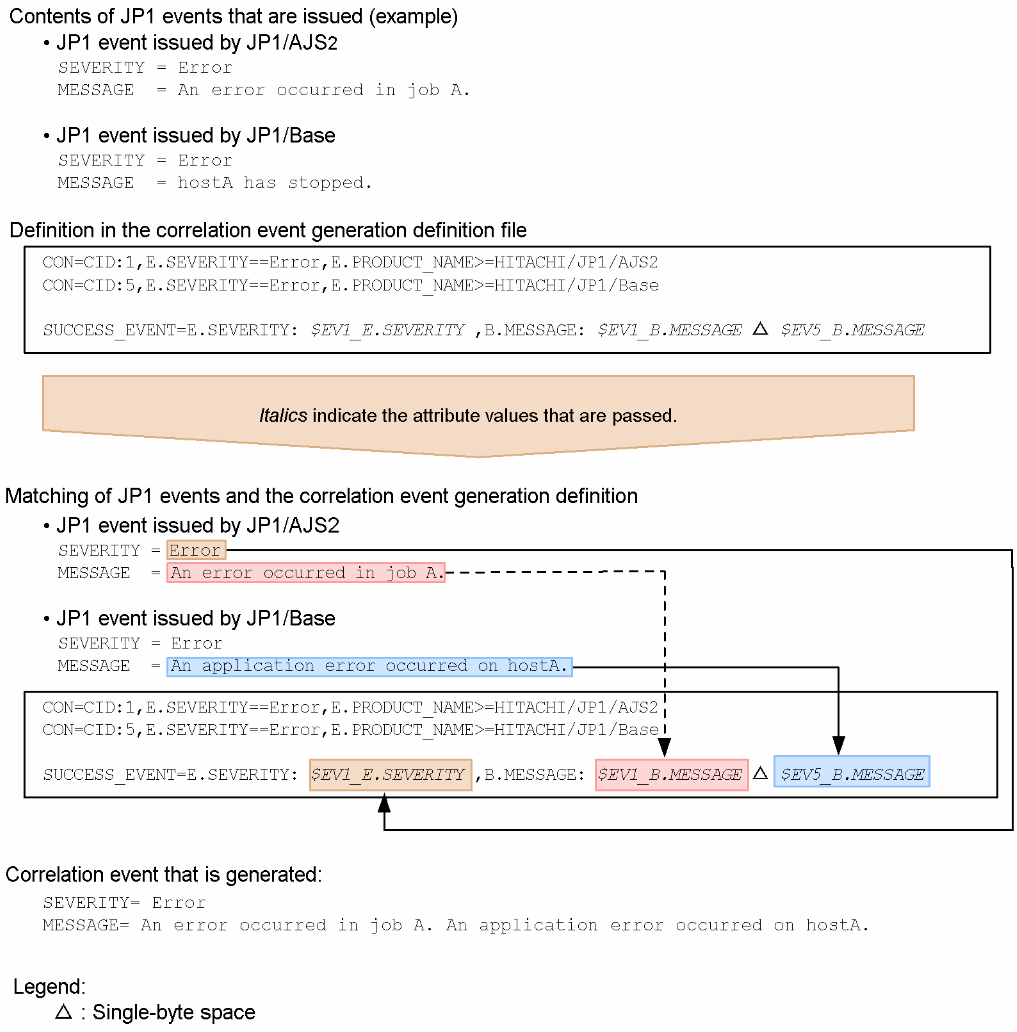
This value is obtained by converting the JP1 event's time in GMT to the time zone of JP1/IM - Manager.

#2

You can also specify a JP1 product-specific extended attribute. For example, the program-specific extended attribute for the JP1/AJS job execution host is `E.C0`. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

The following figure shows an example of passing an attribute value from the correlation source event.

Figure 2–4: Example of using a variable to pass an attribute value to the correlation approval event



Contents of JP1 events that are issued (example)

- JP1 event issued by JP1/AJS2

```
SEVERITY = Error
MESSAGE  = An error occurred in job A.
```

- JP1 event issued by JP1/Base

```
SEVERITY = Error
MESSAGE  = hostA has stopped.
```

Definition in the correlation event generation definition file

```
CON=CID:1,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/AJS2
CON=CID:5,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/Base

SUCCESS_EVENT=E.SEVERITY: $EV1_E.SEVERITY ,B.MESSAGE: $EV1_B.MESSAGE △ $EV5_B.MESSAGE
```

Italics indicate the attribute values that are passed.

Matching of JP1 events and the correlation event generation definition

- JP1 event issued by JP1/AJS2

```
SEVERITY = Error
MESSAGE  = An error occurred in job A.
```

- JP1 event issued by JP1/Base

```
SEVERITY = Error
MESSAGE  = An application error occurred on hostA.
```

```
CON=CID:1,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/AJS2
CON=CID:5,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/Base

SUCCESS_EVENT=E.SEVERITY: $EV1_E.SEVERITY ,B.MESSAGE: $EV1_B.MESSAGE △ $EV5_B.MESSAGE
```

Correlation event that is generated:

```
SEVERITY= Error
MESSAGE= An error occurred in job A. An application error occurred on hostA.
```

Legend:

△ : Single-byte space

In this example, the event levels issued by JP1/AJS and JP1/Base associate the JP1 event for an error, resulting in generation of a correlation event.

This example defines *correlation-approval-event* as follows:

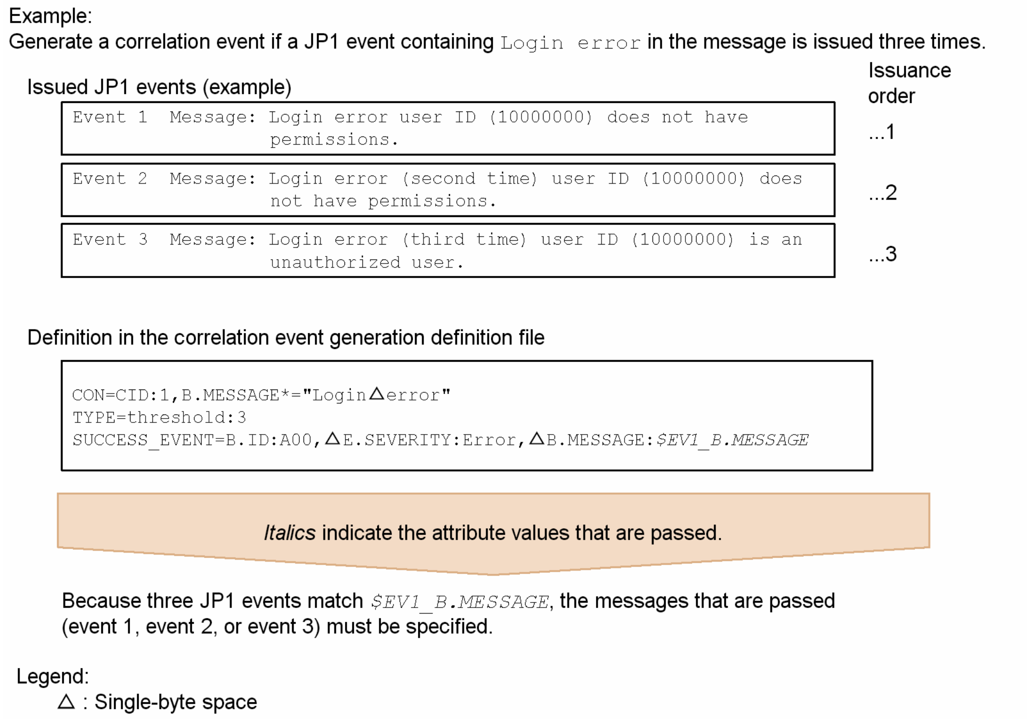
- For the event level, the correlation event passes the event level of the JP1 event issued by JP1/AJS.
- For the message, the correlation event passes the messages for the JP1 events issued by JP1/AJS and JP1/Base.

(b) Passing an attribute value of the correlation source event to an attribute value of the correlation event (when the event correlation type is threshold)

This subsection describes how to define a correlation approval event using a variable when the event correlation type is threshold.

When the event correlation type is threshold, multiple JP1 events can satisfy a single event condition (CON). The following figure shows an example.

Figure 2–5: When the event correlation type is threshold



Example:
Generate a correlation event if a JP1 event containing `Login error` in the message is issued three times.

Issued JP1 events (example)

	Issuance order
`Event 1  Message: Login error user ID (10000000) does not have permissions.`	...1
`Event 2  Message: Login error (second time) user ID (10000000) does not have permissions.`	...2
`Event 3  Message: Login error (third time) user ID (10000000) is an unauthorized user.`	...3

Definition in the correlation event generation definition file

```
CON=CID:1,B.MESSAGE*="Login△error"
TYPE=threshold:3
SUCCESS_EVENT=B.ID:A00,△E.SEVERITY:Error,△B.MESSAGE:$EV1_B.MESSAGE
```

Italics indicate the attribute values that are passed.

Because three JP1 events match *$EV1_B.MESSAGE*, the messages that are passed (event 1, event 2, or event 3) must be specified.

Legend:
△ : Single-byte space

As shown in this figure, three JP1 events (`Event 1`, `Event 2`, and `Event 3`) match `$EV1_B.MESSAGE`. Therefore, the message to be passed must be specified.

In this case, specify the correlation approval event in the following format:

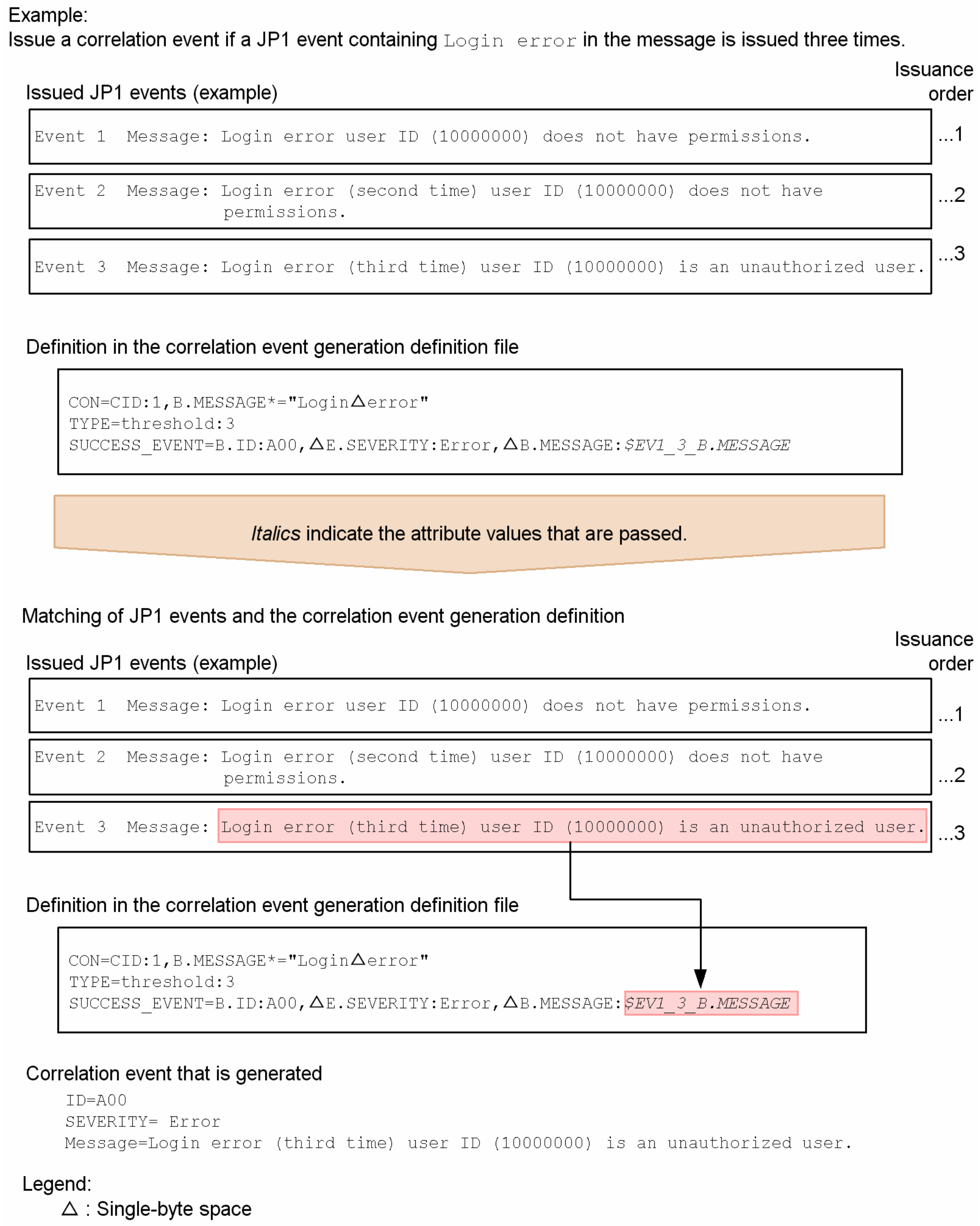
- `SUCCESS_EVENT=`*attribute-name*`:$EV`*n*`_`*m*`_`*attribute-name*

For *n*, specify the condition ID (`CID`) that was specified in the event condition as described above. For the right-hand *attribute-name*, specify the attribute that is to be passed from the correlation source event. Note that if the event ID (`B.ID`) is specified in the left-hand *attribute-name*, an attribute value of the correlation source event cannot be passed.

In *m*, specify the order in which the JP1 events (correlation source events) are processed. To pass the attribute value of the third JP1 event that was processed, specify 3 in *m*. If the value of *m* is greater than the value specified in the threshold (`threshold:`*n*), a definition error results.

The following figure shows an example of passing attribute values when the event correlation type is threshold.

Figure 2–6: Example of passing attribute values when the event correlation type is threshold



Example:
Issue a correlation event if a JP1 event containing `Login error` in the message is issued three times.

Issued JP1 events (example)
Issuance order

```
Event 1  Message: Login error user ID (10000000) does not have permissions.     ...1
Event 2  Message: Login error (second time) user ID (10000000) does not have    ...2
                  permissions.
Event 3  Message: Login error (third time) user ID (10000000) is an unauthorized user.  ...3
```

```
CON=CID:1,B.MESSAGE*="Login△error"
TYPE=threshold:3
SUCCESS_EVENT=B.ID:A00,△E.SEVERITY:Error,△B.MESSAGE:$EV1_3_B.MESSAGE
```

Italics indicate the attribute values that are passed.

Matching of JP1 events and the correlation event generation definition
Issued JP1 events (example)
Issuance order

```
Event 1  Message: Login error user ID (10000000) does not have permissions.     ...1
Event 2  Message: Login error (second time) user ID (10000000) does not have    ...2
                  permissions.
Event 3  Message: Login error (third time) user ID (10000000) is an unauthorized user.  ...3
```

```
CON=CID:1,B.MESSAGE*="Login△error"
TYPE=threshold:3
SUCCESS_EVENT=B.ID:A00,△E.SEVERITY:Error,△B.MESSAGE:$EV1_3_B.MESSAGE
```

```
ID=A00
SEVERITY= Error
Message=Login error (third time) user ID (10000000) is an unauthorized user.
```

You can omit both *n* and *m* in *attribute-name* : `$EV`*n*`_`*m*`_`*attribute-name*. The following examples describe how attribute values are passed when *n* and *m* are omitted.

Example 1:

If a JP1 event containing `Login error` in the message is issued three times, generate a correlation event that receives the message in the correlation source event.

Definition in the correlation event generation definition file

```
[ex.1]
CON=CID:1,B.MESSAGE*="Login error"
TYPE=threshold:3
SUCCESS_EVENT=B.ID:A00,E.SEVERITY:Error,B.MESSAGE:setting
```

Table 2–51: Conditions to be satisfied and settings (in Example 1)

No.	Condition to be satisfied	Setting
1	Pass to the correlation event the message in the first JP1 event that satisfies the event condition	$EV1_1_B.MESSAGE or $EV_1_B.MESSAGE
2	Pass the message in the second JP1 event that satisfies the event condition	$EV1_2_B.MESSAGE or $EV_2_B.MESSAGE
3	Pass the message in the third (last) JP1 event that satisfies the event condition	$EV1_3_B.MESSAGE, $EV1_B.MESSAGE, $EV_3_B.MESSAGE, or $EV_B.MESSAGE

Example 2:

If a JP1 event that satisfies either of the conditions listed below is issued 10 times, generate a correlation event that receives the message in the correlation source event.

- Event ID is `100` and the message contains `Warning`.
- Event ID is `200` and the message contains `Warning` or `Error`.

Definition in the correlation event generation definition file:

```
[ex.2]
CON=CID:100,B.ID==100,B.MESSAGE*="Warning"
CON=CID:200,B.ID==200,B.MESSAGE*="Warning";"Error"
TYPE=threshold:10
SUCCESS_EVENT=B.ID:B00,E.SEVERITY:Error,B.MESSAGE:setting
```

Table 2–52: Conditions to be satisfied and settings (in Example 2)

No.	Condition	Setting
1	Pass to the correlation event the message in the first JP1 event that satisfies the event condition (condition ID: 100)	$EV100_1_B.MESSAGE
2	Pass to the correlation event the message in the fifth JP1 event that satisfies the event condition (condition ID: 100)	$EV100_5_B.MESSAGE
3	Pass to the correlation event the message in the 10th JP1 event that satisfies the event condition (condition ID: 100)	$EV100_10_B.MESSAGE
4	Pass to the correlation event the message in the first JP1 event processed, regardless of the event conditions	$EV_1_B.MESSAGE
5	Pass to the correlation event the message in the fifth JP1 event processed, regardless of the event conditions	$EV_5_B.MESSAGE
6	Pass to the correlation event the message in the 10th (last) JP1 event processed, regardless of the event conditions	$EV_10_B.MESSAGE or $EV_B.MESSAGE

The following summarizes the processing:

When n is omitted:

If *n* is omitted, only the correlation source event with the order specified in *m* is used for checking the conditions. For example, if 3 is specified in *m*, the attribute value of the third correlation source event processed is passed to the correlation event.

When m is omitted:

If *m* is omitted, the last correlation source event processed is the target, regardless of the order. For example, if the threshold is 10, the attribute value of the 10th correlation source event processed is passed.

If *n* is specified, the attribute value of the last correlation source event processed by the event condition is passed.

When n and m are both omitted:

If *n* and *m* are both omitted, the last correlation source event processed is the target, regardless of the event conditions or the order of processing.

Note that regardless of whether *n* or *m* is specified, if no (source) JP1 event satisfies the conditions, the variable is replaced with the null character (0 bytes).

(c) Passing part of an attribute value of the correlation source event to the correlation event

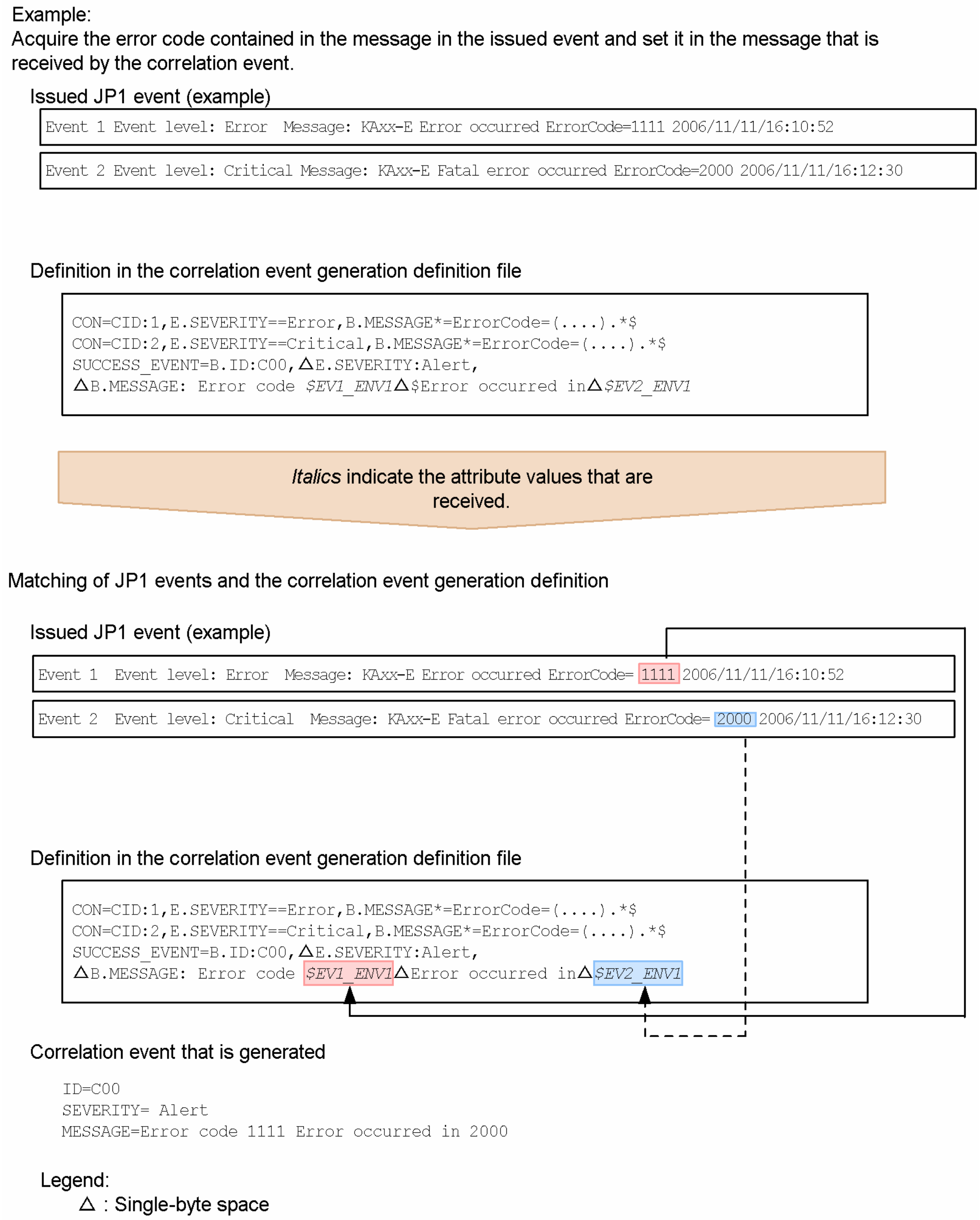
To pass part of an attribute value of the correlation source event to the correlation event, use the `$EV`*n*`_ENV`*o* variable. In this case, use a regular expression (`*=`) to specify the event condition and enclose the part of the attribute value that is to be acquired in parentheses.

Specify *correlation-approval-event* in the following format:

`SUCCESS_EVENT=`*attribute-name*`:$EV`*n*`_ENV`*o*

Specify the correlation source event to be received by `CID` and specify the value of `CID` in *n*. In *o* of `ENV`*o*, specify the acquisition order. The following figure shows an example of receiving part of an attribute value.

Figure 2–7: Example of receipt by the correlation approval event when the $EVn_ENVo variable is used



Example:
Acquire the error code contained in the message in the issued event and set it in the message that is received by the correlation event.

Issued JP1 event (example)

```
Event 1 Event level: Error  Message: KAxx-E Error occurred ErrorCode=1111 2006/11/11/16:10:52
Event 2 Event level: Critical Message: KAxx-E Fatal error occurred ErrorCode=2000 2006/11/11/16:12:30
```

Definition in the correlation event generation definition file

```
CON=CID:1,E.SEVERITY==Error,B.MESSAGE*=ErrorCode=(....).*$
CON=CID:2,E.SEVERITY==Critical,B.MESSAGE*=ErrorCode=(....).*$
SUCCESS_EVENT=B.ID:C00,△E.SEVERITY:Alert,
△B.MESSAGE: Error code $EV1_ENV1△$Error occurred in△$EV2_ENV1
```

Italics indicate the attribute values that are received.

Matching of JP1 events and the correlation event generation definition

Issued JP1 event (example)

```
Event 1  Event level: Error  Message: KAxx-E Error occurred ErrorCode= 1111 2006/11/11/16:10:52
Event 2  Event level: Critical  Message: KAxx-E Fatal error occurred ErrorCode= 2000 2006/11/11/16:12:30
```

Definition in the correlation event generation definition file

```
CON=CID:1,E.SEVERITY==Error,B.MESSAGE*=ErrorCode=(....).*$
CON=CID:2,E.SEVERITY==Critical,B.MESSAGE*=ErrorCode=(....).*$
SUCCESS_EVENT=B.ID:C00,△E.SEVERITY:Alert,
△B.MESSAGE: Error code $EV1_ENV1△Error occurred in△$EV2_ENV1
```

Correlation event that is generated

```
ID=C00
SEVERITY= Alert
MESSAGE=Error code 1111 Error occurred in 2000
```

Legend:
△ : Single-byte space

This example uses parentheses to acquire the right-hand term of `ErrorCode=` from the correlation source event that is specified by the conditions of condition ID (`CID`) =1 and condition ID (`CID`) =2.

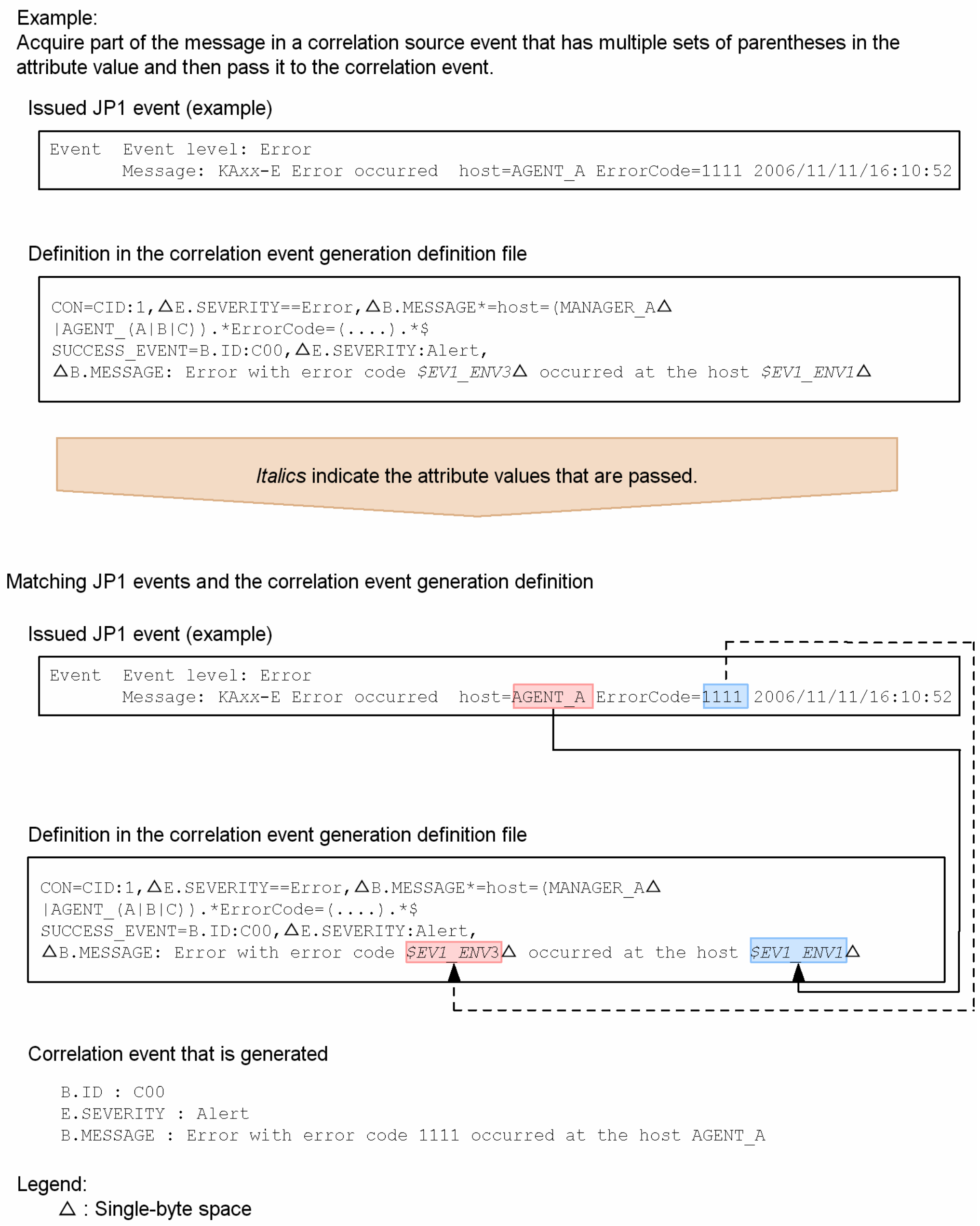
If you use the `$EV`*n*`_ENV`*o* variable, when a correlation source event that has an attribute value containing a specific character string is issued, you can generate a correlation event, and then pass the portion of the character string contained in the attribute value to the correlation event.

In this case, specify in *o* of `ENV`*o* the numeric value that determines the parentheses pair that follows the regular expression (`*=`) specified in the event conditions. In other words, count parentheses pairs from left to right for the attribute value in the correlation source event that follows the regular expression (`*=`) in the event conditions, and then specify in *o* the location that is to be passed.

The part acquired by `$EV`*n*`_ENV`*o* is the same as when `$EV`*n*`_ENV`*o* is specified in the duplicate attribute value condition. For details, see *Figure 2-3 Correspondence between the event condition (CON) and the part that is acquired by $EVn_ENVo*.

The example shown below generates a correlation event if a correlation source event with an attribute value that contains a specific character string is issued, and passes part of the character string contained in that attribute value to the correlation event.

Figure 2–8: Example of passing part of a character string contained in an attribute value to the correlation event



Example:
Acquire part of the message in a correlation source event that has multiple sets of parentheses in the attribute value and then pass it to the correlation event.

Issued JP1 event (example)

```
Event  Event level: Error
       Message: KAxx-E Error occurred  host=AGENT_A ErrorCode=1111 2006/11/11/16:10:52
```

Definition in the correlation event generation definition file

```
CON=CID:1,△E.SEVERITY==Error,△B.MESSAGE*=host=(MANAGER_A△
|AGENT_(A|B|C)).*ErrorCode=(....).*$
SUCCESS_EVENT=B.ID:C00,△E.SEVERITY:Alert,
△B.MESSAGE: Error with error code $EV1_ENV3△ occurred at the host $EV1_ENV1△
```

Italics indicate the attribute values that are passed.

Matching JP1 events and the correlation event generation definition

Issued JP1 event (example)

```
Event  Event level: Error
       Message: KAxx-E Error occurred  host=AGENT_A ErrorCode=1111 2006/11/11/16:10:52
```

Definition in the correlation event generation definition file

```
CON=CID:1,△E.SEVERITY==Error,△B.MESSAGE*=host=(MANAGER_A△
|AGENT_(A|B|C)).*ErrorCode=(....).*$
SUCCESS_EVENT=B.ID:C00,△E.SEVERITY:Alert,
△B.MESSAGE: Error with error code $EV1_ENV3△ occurred at the host $EV1_ENV1△
```

Correlation event that is generated

```
B.ID : C00
E.SEVERITY : Alert
B.MESSAGE : Error with error code 1111 occurred at the host AGENT_A
```

Legend:
△ : Single-byte space

This example specifies the definition in such a manner that whenever a correlation source event that satisfies the conditions listed below is generated, an attribute value is passed from it to the correlation event:

- `host=` is followed by `MANAGER_A`, `AGENT_A`, `AGENT_B`, or `AGENT_C`.
- `ErrorCode=` is followed by a character string of at least 4 characters.#

#

- If the character string consists of more than four characters, only the first four characters are passed.
  For example, in the case of `ErrorCode=12345678`, `1234` is passed.

- If the character string consists of fewer than four characters, the necessary number of characters that follow `ErrorCode=` *character-string* are included so that four characters are passed.

  For example, in the case of `ErrorCode=1 2006/11/11`, `1 20` is passed.

If the character string that follows `ErrorCode=` consists of fewer than 4 characters, no correlation event is generated.

Example definition

Example 1: Generate a correlation event for any JP1 event whose event level is `Error` or higher:

```
VERSION=2

#Generate a correlation event for any a JP1 event
#whose event level is Error or higher
[filter_over_error]
CON=CID:1,B.ID==1,E.SEVERITY==Error;Critical;Alert;Emergency
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

Example 2: Generate a correlation event for any JP1 event whose event level is `Error` or higher and for any JP1 event issued by JP1/AJS whose event level is `Error`:

If the following definition is specified and JP1/AJS issues a JP1 event whose event level is `Error`, two correlation events will be generated because the JP1 event satisfies the two correlation event generation conditions `over_error` and `ajs2_over_error`:

```
VERSION=2

#Generate a correlation event for any JP1 event whose
#event level is Error or higher.
[over_error]
CON=CID:1,E.SEVERITY==Error;Critical;Alert;Emergency
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE

#Generate a correlation event for any JP1 event issued by
#JP1/AJS@ whose event level is Error.
[ajs2_over_error]
CON=CID:1,E.SEVERITY==Error,E.PRODUCT_NAME==/HITACHI/JP1/AJS2
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

To generate only one correlation event when JP1/AJS issues a JP1 event whose event level is `Error`, specify the first correlation event generation condition as follows:

```
VERSION=2

#Generate a correlation event for any JP1 event whose
#event level is Error or higher.
#Exclude events issued by JP1/AJS2.
[over_error_and_not_ajs2]
CON=NOT,E.SEVERITY==Error,E.PRODUCT_NAME==/HITACHI/JP1/AJS2
CON=CID:1,E.SEVERITY==Error;Critical;Alert;Emergency
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE

#Generate a correlation event for any JP1 event issued by
#JP1/AJS2 whose event level is Error.
[ajs2_over_error]
```

```
CON=CID:1,E.SEVERITY==Error,E.PRODUCT_NAME==/HITACHI/JP1/AJS2
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

Example 3: Define a timeout period:

```
VERSION=2

[condition]
CON=NOT,E.SEVERITY==Error,E.PRODUCT_NAME==/HITACHI/JP1/AJS2

CON=CID:1,B.ID==1,B.MESSAGE==TEST,E.SEVERITY==Warning
CON=CID:2,B.ID==1,B.MESSAGE==TEST,E.SEVERITY==Error
CON=CID:3,B.ID==1,B.MESSAGE==TEST,E.SEVERITY==Critical

TIMEOUT=10
SUCCESS_EVENT=E.SEVERITY:Emergency,B.MESSAGE:$EV1_B.MESSAGE
```

Example 4: Generate a single correlation event that combines the messages in JP1 events issued by JP1/AJS2 and JP1/Base and whose event level is `Error`:

```
VERSION=2

[cond1]

CON=CID:1,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/AJS2
CON=CID:5,E.SEVERITY==Error,E.PRODUCT_NAME>=HITACHI/JP1/Base

SUCCESS_EVENT=E.SEVERITY:$EV1_E.SEVERITY,B.MESSAGE:"$EV1_B.MESSAGE $EV5_B.
MESSAGE"
```

Example 5: Acquire a value by using the `$EV`*n*`_ENV`*o* variable:

This example acquires the detail code `errorΔcodeΔ=`Δ*n*Δ that is included in the message and then places it in the message in the correlation event (*n*: any character string; Δ: Space).

```
VERSION=2

[SAMPLE]

CON=CID:100, B.MESSAGE*=(errorΔcodeΔ=.*Δ)
SUCCESS_EVENT=B.ID:100,E.SEVERITY:Emergency,B.MESSAGE: error-information[$
EV100_ENV1Δ]
```

Example 6: Narrow down the target range for correlation by the host and generate a correlation event for each user with the maximum correlation number set to 20:

```
VERSION=2

[condition2]
TARGET=B.SOURCESERVER==host1;host2;host3
CON=NOT, E.SEVERITY==Error, E.PRODUCT_NAME==/HITACHI/JP1/AJS2

CON=CID:1, B.ID==1, B.MESSAGE==TEST, E.SEVERITY==Warning
CON=CID:2, B.ID==1, B.MESSAGE==TEST, E.SEVERITY==Error
CON=CID:3, B.ID==1, B.MESSAGE==TEST, E.SEVERITY==Critical

SAME_ATTRIBUTE=E.USERNAME
CORRELATION_NUM=20
```

```
TIMEOUT=10
SUCCESS_EVENT=B.MESSAGE:$EV1_B.MESSAGE
```

Correlation event generation environment definition file

Format

```
[logical-host-name\JP1CONSOLEMANAGER\EVGEN]
"OPERATION_LOG_SIZE"=dword:hexadecimal-value
"OPERATION_LOG_NUM"=dword:hexadecimal-value
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines the size and number of correlation event generation history files.

When this file is updated, the definition information is updated for all processes managed by JP1/IM - Manager.

When the definitions are applied

The definition takes effect when JP1/IM - Manager is restarted or the `jco_spmd_reload` command is executed after the `jbssetcnf` command has been executed to apply the definition to the common definition information.

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER\EVGEN]`

Specifies the key name for the JP1/IM - Manager environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"OPERATION_LOG_SIZE"=dword:`*hexadecimal-value*

Specifies in hexadecimal notation the size of one correlation event generation history file. The permitted value range is from 00010000 to 06400000 (from 64 kilobytes to 100 megabytes). The default is `00A00000`.

`"OPERATION_LOG_NUM"=dword:`*hexadecimal-value*

Specifies in hexadecimal notation the number of correlation event generation history files. The permitted value range is from 00000003 to 00000064 (from 3 to 100 files). The default is `00000003` (3 files).

How to determine the size and number of correlation event generation history files

If it is necessary to adjust the size and number of correlation event generation history files, estimate the size of the correlation event generation history file required for one day and multiply that value by the number of days the files are to be retained. Set a value that is larger than the estimated value.

For details about the estimation, see the Release Notes for JP1/IM - Manager.

Definition file for manually registering incidents (incident.conf)

Format

```
VERSION=version-information
SS_MODE={1|2|3}

#comment-line
[SS_URL=http://JP1/Service Support host:port-number]
```

File

`incident.conf` (definition file for manually registering incidents)

`incident.conf.model` (model file for the definition file for manually registering incidents)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\incident\`

For a logical host:

shared-folder`\jp1cons\conf\console\incident\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/incident/`

For a logical host:

shared-directory`/jp1cons/conf/console/incident/`

Description

This definition file is used to register a JP1 event in JP1/IM - View as an incident in another product.

When the definitions are applied

The settings in the definition file for manually registering incidents take effect when the `jco_spmd_reload` command is executed, or when a user logs in to JP1/IM - Manager (Central Console) after restarting JP1/IM - Manager.

Information that is specified

`VERSION=`*version-information*

Specify the version of the definition file for manually registering incidents. Specify `3` for *version-information*. If you omit this parameter, or did not specify the value correctly, the `SS_URL` and `SS_MODE` parameters are ignored. Note that if you specify this parameter more than once, the parameter on the last line is valid.

Table 2–53: List of parameters that can be specified for the version information and definition file for manually registering incidents

Version information	Parameter name
2	`SS_URL`#

Version information	Parameter name
3	SS_URL SS_MODE

#

This works with SS_MODE=1.

SS_MODE={1|2|3}

Specify the registration mode of an incident. If you want to specify this parameter, specify 3 for the VERSION parameter. If not, this parameter is ignored. You can specify 1, 2, or 3. The following table describes available incident registration modes and when each mode should be used.

Table 2–54: Incident registration modes and when to use each of them

Incident registration mode	Description	When to use	Supported version of JP1/IM - Manager, JP1/IM - View, and JP1/ Service Support
SS_MODE=1	Source attributes and their target fields are fixed.	The specification of JP1/IM - Manager 10-00 or earlier must be used for linkage with JP1/Service Support.	09-50 or later
SS_MODE=2	• Source attributes and their target fields are fixed. • The event ID (B.IDBASE) is inherited in addition to the attributes that are inherited when SS_MODE=1.	• The event ID is required to be registered. • Linkage with JP1/IM - Manager, JP1/ Service Support, and JP1/Navigation Platform is required.	10-10 or later
SS_MODE=3	• The mapping between source attributes and target fields is configurable. • Multiple attributes can be mapped to one target field. • Any character string you want can be inherited.	• Any attribute or character string you want is required to be registered. • This mode also allows linkage with JP1/IM - Manager, JP1/Service Support, and JP1/ Navigation Platform.	11-50 or later

If you omit this parameter, or do not specify the value correctly, 1 is assumed. Note that if you specify this parameter more than once, the parameter on the last line is valid.

If you specify the registration mode of an incident, information to be registered as an incident is changed. For details about registration modes of incidents and information to be registered as incidents, see *10.1.1 Attributes of a JP1 event registered as an incident in JP1/Service Support during linkage* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

#*comment-line*

A line beginning with a hash mark (#) is treated as a comment.

[SS_URL=http://*JP1/Service Support-host*:*port-number*]

Specifies the URL of a Web page for JP1/Service Support on which you can register an incident by using one-byte numeric values and symbols. The default is SS_URL=, and no value is set.

The maximum length of a URL that calls JP1/Service Support is 2,046 characters. If 2 is set for the registration mode of an incident, event IDs are inherited. Therefore, the length of a message that can be inherited when 2 is set is less than the length of a message when 1 is set. If a message is truncated before the end, the user must copy the rest of the message displayed in the Event Details window, and paste it into JP1/Service Support.

When you code the port numbers of JP1/Service Support in this parameter, you must set them to ensure passage through the firewall between the JP1/IM - View machine and the JP1/Service Support machine.

To link with JP1/Service Support after upgrading JP1/IM - Manager, add this line, and then do the following:

- Change *version-information* to `2` or `3`.
- Add `SS_MODE` on a new line to specify the registration mode when you want to register an event ID (`SS_MODE=2`) or you want a desired attribute or character string of a JP1 event to be inherited as an incident (`SS_MODE=3`).
- Change the line beginning with `IDM_URL` as the comment statement (add `#`).

Restart JP1/IM - Manager or execute the `jco_spmd_reload` command to apply the definitions. If you already logged in to JP1/IM - View, restart JP1/IM - View.

Configuration file for incident inheritance information (incident_info.conf)

Format

```
[@encode UTF-8]
#item-field-ID=value-to-be-set-for-the-item
JP1/Service-Support-item-element-ID=value-passed-to-item-element[end-of-line
-character]
```

File

`incident_info.conf` (Configuration file for incident inheritance information)

`incident_info.conf.model` (Model file for the configuration file for incident inheritance information)

Storage directory

In Windows:

Physical hosts:

Console-path`\conf\console\incident\`

Logical hosts:

shared-folder`\jp1cons\conf\console\incident\`

In UNIX:

Physical hosts:

`/etc/opt/jp1cons/conf/console/incident/`

Logical hosts:

shared-directory`/jp1cons/conf/console/incident/`

Description

Attributes or character strings of a JP1 event can be inherited as an incident in JP1/Service Support. This file defines which attributes or character strings of a JP event are mapped to which item elements of the New item window in JP1/Service Support.

When the definitions are applied

The settings edited in the configuration file for incident inheritance information take effect when you log in to JP1/IM - Manager (Central Console) with JP1/IM - View after setting the incident registration mode to 3 and then executing the `jco_spmd_reload` command or restarting JP1/IM - Manager.

Information that is specified

`[@encode UTF-8]`

Specifies the character encoding of the configuration file for incident inheritance information. The `@encode` statement must be on the first line. When the `@encode` statement does not exist, the character encoding of the manager is used. The acceptable character encoding is UTF-8. When the specified character encoding is UTF-8, the character encoding of the configuration file is set to UTF-8.

The error message KAVB1115-W is issued and the character encoding of the manager is used when any of the following conditions is true:

- The configuration file does not begin with `@encode`.
- `@encode` is not followed by a character encoding value.

The error message KAVB1119-W is issued and the character encoding of the manager is used when the following condition is true:

- The specified character encoding is not UTF-8.

The managers use the following character encodings:

In Windows:

One of the following character encodings is used depending on the system locale:

Japanese: MS932 (Note that available characters are limited to SJIS characters.)

English: C

Chinese: GB18030

Any encoding other than Japanese or Chinese: C

In UNIX:

The character encoding depends on the value of the `LANG` environment variable specified in the `/etc/opt/jp1cons/conf/jp1co_env.conf` file.

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

JP1/Service-Support-item-element-ID=value-passed-to-item-element`[`*end-of-line-character*`]`

Specifies which attributes or character strings of a JP1 event that are inherited as incidents are mapped to which item elements of the New item window in JP1/Service Support.

JP1/Service-Support-item-element-specification-ID

Specifies an item element specification ID in JP1/Service Support. If there are multiple occurrences of the same ID, the first occurrence takes precedence. For details about item element specification IDs, see the *JP1/Service Support Configuration and Administration Guide*.

value-passed-to-item-element`[`*end-of-line-character*`]`

Specifies any character strings or variables. You can specify as many multiple variables as you need.

A character string can consist of any characters other than control characters. When you include a control character (0x00 to 0x0F, 0x14 to 0x1F, or 0x7F), the character is replaced with a space (0x20). To use a dollar sign (`$`) as a literal character, place an escape character `\` immediately before the dollar sign (`$`). To break a line, specify `\n` on the point where you want to break the line. To use `\n` as literal characters, specify `\\n`.

The following table describes how to specify a variable.

Table 2–55: How to specify a variable

Format	Description
`$`*variable-name*	A variable must be specified in the following format: `$`*variable-name*. For details about specific variable names of JP1 event attributes, see *Table 2-57 Variables that can be specified for JP1/Service Support item elements*.
`${`*variable-name*`}`	A variable name must be enclosed in curly brackets (`{ }`) when the variable name is directly followed by an alphanumeric character or an underscore (_).

`$`*variable-name*`$URLENC`
`${`*variable-name*`$URLENC}`
	The attribute value is URL-encoded with UTF-8 character encoding.

`$`*variable-name*`$ENC`
`${`*variable-name*`$ENC}`
	The attribute value is Base64-encoded.

Format	Description
$*variable-name*$ENC$URLENC ${*variable-name*$ENC$URLENC}	The attribute value is Base64-encoded and then URL-encoded.

The following table lists the examples of specified variables. These examples assume that the value of the event ID ($EVID) is 100:0 and the value of the EX extended attribute ($EV"EX") is ABC.

Table 2–56: Examples of specified variables

Specified variable	Converted value
$EVID abc	100:0 abc
$EVIDabc	In Windows $EVIDabc In UNIX Converted to an empty string.
${EVID}abc	100:0abc
$EVID_abc	In Window $EVID_abc In UNIX Converted to an empty string.
${EVID}_abc	100:0_abc
$EV"EX" abc	ABC abc
$EV"EX"abc	ABCabc

The table below lists variables that can be used to pass the attribute values. You can map any source attribute to any target element but you must ensure that the value of the source attribute matches the display format of the target element.

Table 2–57: Variables that can be specified for JP1/Service Support item elements

Item	Information to be inherited	Variable name
Entire basic event information	Entire basic event information	EVBASE
Event ID (*basic-code*:*extended-code*)	Value of the event ID in the format *basic-code*:*extended-code*. *basic-code* is the value of the event ID (B.ID). *extended-code* is the value of the event code (extended code) (B.IDEXT). Both *basic-code* and *extended-code* are an 8-digit hexadecimal number (where A-F are uppercase). Zeros preceding the ID are omitted. When the extended code is 00000000, the value of the variable is *basic-code*:0.	EVID
Event ID (*basic-code*)	8-digit hexadecimal number representing the event ID (basic code) (where A-F are uppercase). Zeros preceding the ID are omitted.	EVIDBASE
Event registration date	Character value of the registration time (B.TIME) in the following format: *yyyy*/*mm*/*dd*	EVDATE
Event registration time (*hh*:*mm*:*ss*)	Character value of the registration time (B.TIME) in the following format: *hh*:*mm*:*ss*	EVTIME
Event source process ID	Value of B.PROCESSID	EVPID
User ID of the event source process	Value of B.USERID	EVUSRID

Item	Information to be inherited	Variable name
Group ID of the event source process	Value of B.GROUPID	EVGRPID
Event source user name	Value of B.USERNAME	EVUSR
Event source group name	Value of B.GROUPNAME	EVGRP
Event source server name	Value of B.SOURCESERVER Only when the event source host mapping is disenabled	EVHOST
Event source IP address	Value of B.SOURCEIPADDR	EVIPADDR
Event database serial number	Value of B.SEQNO	EVSEQNO
Event arrival date	Character value of the arrival time (B.ARRIVEDTIME) in the following format: *yyyy*/*mm*/*dd*	EVARVDATE
Event arrival time	Character value of the arrival time (B.ARRIVEDTIME) in the following format: *hh*:*mm*:*ss*	EVARVTIME
Event database serial number at the event source	Value of B.SOURCESEQNO	EVSRCNO
Message	Value of B.MESSAGE	EVMSG
Detailed information	Character value of the detailed information (B.DETAIL) in the following format: *informaion-1*Δ*informaion-2*Δ*informaion-3*Δ...*informaion-n*Δ (where Δ indicates a space)	EVDETAIL
Severity level	Value of E.SEVERITY	EVSEV
User name	Value of E.USER_NAME	EVUSNAM
Object type	Value of E.OBJECT_TYPE	EVOBTYP
Object name	Value of E.OBJECT_NAME	EVOBNAM
Root object type	Value of E.ROOT_OBJECT_TYPE	EVROBTYP
Root object name	Value of E.ROOT_OBJECT_NAME	EVROBNAM
Product name	Value of E.PRODUCT_NAME	EV"PRODUCT_NAME"
Object ID	Value of E.OBJECT_ID	EV"OBJECT_ID"
Occurrence	Value of E.OCCURRENCE	EV"OCCURRENCE"
Start time	Value of E.START_TIME	EV"START_TIME"
End time	Value of E.END_TIME	EV"END_TIME"
Return code	Value of E.RESULT_CODE	EV"RESULT_CODE"
Event source host name	Value of E.JP1_SOURCEHOST Only when the event source host mapping is enabled	EV"JP1_SOURCEHOST"
Any extended attribute	Value of a named extended attribute	EV"extended-attribute-name"
Correlation event flag	Value of E.@JP1IM_CORRELATE Not a correlation event: 0 Correlation approval event: 1 Correlation failure event: 2	EV"@JP1IM_CORRELATE"

Item	Information to be inherited	Variable name
	Only when the correlation event generation function is enabled and the integrated monitoring database is enabled	
Original severity level	Value of E.@JP1IM_ORIGINAL_SEVERITY Only when the severity changing function is enabled	EV"@JP1IM_ORIGINAL_SEVERITY"
New severity level flag	Value of E.@JP1IM_CHANGE_SEVERITY Severity is not changed: 0 Severity is changed: 1 Only when the severity changing function is enabled	EV"@JP1IM_CHANGE_SEVERITY"
Changed display message	Value of E.@JP1IM_DISPLAY_MESSAGE Only when the display message change function is enabled	EV"@JP1IM_DISPLAY_MESSAGE"
New display message flag	Value of E.@JP1IM_CHANGE_MESSAGE Message is not changed: 0 Message is changed: 1 Only when the display message change function is enabled	EV"@JP1IM_CHANGE_MESSAGE"
Memo	Value of E.@JP1IM_MEMO An attribute that is set after memo is set	EV"@JP1IM_MEMO"
Common exclude conditions group ID	Value of E.JP1_IMCOMEXCLUDE_ID Only when the extended mode of common exclusion is enabled and the integrated monitoring database is enabled	EV"JP1_IMCOMEXCLUDE_ID"
Common exclude conditions group name	Value of E.JP1_IMCOMEXCLUDE_NAME Only when the extended mode of common exclusion is enabled and the integrated monitoring database is enabled	EV"JP1_IMCOMEXCLUDE_NAME"
Common exclude conditions group target-for-exclusion	Value of E.JP1_IMCOMEXCLUDE_TARGET Only when the extended mode of common exclusion is enabled and the integrated monitoring database is enabled	EV"JP1_IMCOMEXCLUDE_TARGET"

When a variable name other than those listed above is specified, the statement including the variable is not replaced with event information. For example, when you use the variable AAA to compose the statement $AAA, the literal characters $AAA are passed to the New item window in JP1/Service Support.

When the value of an attribute that is specified in EV"*extended-attribute-name*" is not available, the statement including the variable is not replaced with event information. For example, when you specify the statement $EV"BBB" but the JP1 event does not have the extended attribute BBB, the literal characters $EV"BBB" are passed to the New item window in JP1/Service Support.

When the value of an attribute that is specified in a statement other than EV"*extended-attribute-name*" is not available, the statement including the variable is replaced with an empty string. For example, when you specify the statement $EVSEV but the JP1 event does not have the extended attribute SEVERITY, "" (an empty string) is passed to the New item window in JP1/Service Support.

Example definition

To show "Event that occurred on *event-source-host name* (*IP-address*): *event-ID*" in the **Title** element of the New item window in JP1/Service Support (only when the event source host mapping is enabled):

```
TITLE=Event that occurred on $EV"JP1_SOURCEHOST" ($EVIPADDR): $EVIDBASE
```

To show a URL link (by URL-encoding the attribute value with UTF-8 character encoding) in the **Related information** element of the New item window in JP1/Service Support:

```
LINKURL=http://host/page?msg=$EVMSG$URLENC
```

Host information file (jcs_hosts)

Format

```
IP-address host-name-1 host-name-2 host-name-3 ... host-name-8
IP-address host-name-1 host-name-2 host-name-3 ... host-name-8
              :
```

File

`jcs_hosts` (host information file)

`jcs_hosts.model` (model file for the host information file)

Storage directory

In Windows

For a physical host:

Scope-path`\conf\`

For a logical host:

shared-folder`\jp1scope\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1scope/conf/`

For a logical host:

shared-directory`/jp1scope/conf/`

Description

This file defines the host information that is managed by JP1/IM - Manager (Central Scope).

The host information file is used to specify the host information that is used for automatic generation of a monitoring tree and for Host name Comparison during JP1 event collation processing for changing the status of monitoring objects. The format of the host information file is the same as for the `hosts` file.

If `#` is specified, any text following `#` is treated as a comment.

When the definitions are applied

The contents of the host information file take effect when JP1/IM - Manager is restarted or the `jco_spmd_reload` command is executed after the `jcshostsimport` command has been executed.

If you use the `jcshostsimport` command to store the contents of the host information file in the host information database, the host names become all lowercase. Therefore, the host names output by `jcshostsexport` are also in lowercase.

The `jcshostsimport` command does not store comments in the host information file.

Information that is specified

IP-address host-name-1 host-name-2 host-name-3 ... *host-name-8*

Specifies an IP address from the beginning of the line (other than spaces), and then specifies host names or alias names after one or more spaces or tabs.

The maximum length of the IP address is 63 bytes. IP addresses of IP V6 are not supported.

The maximum length of a host name or alias name is 255 bytes.

You can specify a maximum of 8 host names for one IP address and a maximum of 8 IP addresses for one host name.

If the same IP address is specified more than once, the first IP address defined is effective.

If there is a line that contains only an IP address, an error occurs during `jcshostsimport` command execution.

A host name is not case sensitive. Japanese characters cannot be used for a host name. An IP address can also be expressed in hexadecimal notation.

Example definition

```
#
# jcs_hosts
#
# Internet Address Hostname
100.100.10.10     samplehost1  samplehost2
```

Guide information file (jcs_guide.txt)

Format 1

```
DESC_VERSION=1

[EV_GUIDE_number]
NUM=number
EV_COMP_number=attribute-specification:regular-expression
EV_TITLE=character-string
EV_GUIDE=message
[END]
[EV_GUIDE_number]
NUM=number
EV_COMP_number=attribute-specification:regular-expression
EV_TITLE=character-string
EV_GUIDE=message
[END]
   :
```

Format 2

```
DESC_VERSION=2

[EV_GUIDE_number]
NUM=number
EV_COMP_number=attribute-specification:regular-expression
EV_TITLE=character-string
EV_FILE=guide-message-file
[END]
[EV_GUIDE_number]
NUM=number
EV_COMP_number=attribute-specification:regular-expression
EV_TITLE=character-string=character-string
EV_FILE=guide-message-file
[END]
   :
```

File

The guide information file (`jcs_guide.txt`) to be edited depends on the language encoding supported by JP1/IM. The following table shows the correspondence between the language encodings supported by JP1/IM and the guide information files to be edited.

Table 2–58: Correspondence between language encodings supported by JP1/IM and the guide information files

OS	Language type	Language encoding supported by JP1/IM	File to be edited
Windows	Japanese		`jcs_guide_sjis.txt` (guide information file)
			`jcs_guide_sjis.txt.model` (model file for the guide information file)

OS	Language type	Language encoding supported by JP1/IM	File to be edited
	English		`jcs_guide.txt` (guide information file)
			`jcs_guide.txt.model` (model file for the guide information file)
	Chinese		`jcs_guide_GB18030.txt` (guide information file)
UNIX#	Japanese	Shift-JIS encoding	`jcs_guide_sjis.txt` (guide information file)
			`jcs_guide_sjis.txt.model` (model file for the guide information file)
		EUC encoding	`jcs_guide_euc.txt` (guide information file)
			`jcs_guide_euc.txt.model` (model file for the guide information file)
		UTF-8 encoding	`/etc/opt/jp1scope/conf/jcs_guide_UTF-8.txt`
			shared-directory`/jp1scope/conf/jcs_guide_UTF-8.txt`
	English		`jcs_guide.txt` (guide information file)
			`jcs_guide.txt.model` (model file for the guide information file)
	Chinese	GB18030 encoding	`jcs_guide_GB18030.txt` (guide information file)

#: Only files corresponding to the languages supported by the OS exist.

Storage directory

In Windows

For a physical host:

Scope-path`\conf\`

For a logical host:

shared-folder`\jp1scope\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1scope/conf/`

For a logical host:

shared-directory`/jp1scope/conf/`

Description

This file defines guide information about the JP1 events that trigger a change in monitoring object status.

The information specified in this file is displayed in the Guide window of JP1/IM - View.

The maximum size of the guide information file is 1 megabyte.

Format 2 is used to import a user-created TXT or HTML file as the guide-message file and then display it in the Guide window.

If there are multiple matching guide information items, the first item specified in the guide information file is effective.

In Windows, guide information files from version 07-00 of JP1/IM - Manager (Central Scope) can also be read in JP1/IM - Manager version 08-00 and later.

In Windows, guide information files from version 08-00 or later of JP1/IM - Manager can also be read in version 07-00 of JP1/IM - Manager (Central Scope), but the specification `EV_FILE=`*guide-message-file* under `DESC_VERSION=2` is ignored, and the specification `EV_GUIDE=`*message* takes precedence. An error results if the file includes neither specification.

If # is specified, any text following # is treated as a comment. Note that a comment cannot be specified after the start tag, attribute information, or end tag. An error results if a comment is specified following the start and end tags. If a comment is specified following an attribute value, that comment is treated as part of the attribute value.

To use `\`, specify `\\`. If `\` is used in other than `\n` or `\$`, a log is output and the line containing `\` is ignored.

When the definitions are applied

After the guide information file is edited, the definitions in the file take effect when JP1/IM - Manager is restarted or when the `jco_spmd_reload` command is executed.

Information that is specified

`DESC_VERSION=1 | 2`

Specifies the version of the guide information file. The permitted values are 1 and 2.

If you specify the `EV_FILE` parameter to call a guide-message file, you must specify `2` in this parameter.

If you specify `DESC_VERSION=1`, `EV_GUIDE=`*message*, and `EV_FILE=`*guide-message-file* together, the specification of `EV_FILE=`*guide-message-file* will be ignored.

If you specify `DESC_VERSION=2` and also specify both `EV_GUIDE=`*message* and `EV_FILE=`*guide-message-file*, the specification of `EV_FILE=`*guide-message-file* will take precedence.

`[EV_GUIDE_`*number*`]`

This is the start tag for the guide information. The information from the `[EV_GUIDE_`*number*`]` tag to the `[END]` tag constitutes a single definition block. Between this parameter and `[END]`, specify a condition for JP1 events that are to be displayed in the Guide window and the message that is to be displayed. The number begins with 1 and increments by 1 up to the number of guides.

The specification in each instance of the `EV_GUIDE_`*number* tag must be unique. If an invalid character string is specified, a log is output and the corresponding specification is ignored.

If an attribute specified in the `EV_GUIDE_`*number* tag is not permitted, the corresponding specification is ignored.

`NUM=`*number*

Specifies the total number of `EV_COMP_`*number* entries.

`EV_COMP_`*number*`=`*attribute-specification*`:`*regular-expression*

Specifies an attribute to be compared. Specify this parameter for each attribute that is to be compared. The specification in *number* begins with 1 and increments by 1. When multiple parameters have been specified and the AND condition among them is completely satisfied, the message specified in the `EV_GUIDE` parameter is displayed in the Guide window.

The value specified in `EV_COMP_`*number* is ignored if it is less than 1 or greater than the value specified in `NUM=`*number*.

Express the event ID as 8 digits. If you specify `B.ID` as an attribute specification for `EV_COMP_`*number* and you set only the base part of the event ID in the matching condition, you can omit specification of the extended part.

Example:

`EV_COMP_1=B.ID:00004107:00000000` or `EV_COMP_1=B.ID:00004107`

attribute-specification

Specifies an attribute of one the following types:

JP1 event basic attribute: If you specify this type of attribute, use the format `B.`*attribute-name*.

JP1 event extended attribute: If you specify this type of attribute, use the format `E.`*attribute-name*.

Monitoring node attribute: If you specify this type of attribute, you can use the format `T.MONNODEID` (monitoring node ID), with the monitoring node ID expressed as 8 hexadecimal characters.

regular-expression

Specifies a value of the attribute specified in *attribute-specification* using a regular expression. For the regular expression, use an extended regular expression. For details about regular expressions, see *Appendix G. Regular Expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`EV_TITLE=`*character-string*

Specifies the character string that is to be displayed as the title of the Guide window. You can specify this parameter only once between `[EV_GUIDE_`*number*`]` and `[END]`.

`EV_GUIDE=`*message*

Specifies the character string that is to be displayed as a guide message in the Guide window. If you use HTML tags, you can display the guide message in HTML format in the Guide window (for details about the supported HTML tags, see *Table 2-59 HTML tags that can be used in guide messages* in the description of `EV_FILE`). Note that you can specify this parameter only once between `[EV_GUIDE_`*number*`]` and `[END]`.

Express the message as a maximum of 10,240 bytes of characters. If the specified message consists of more than 10,240 bytes, the portion of the message in excess of 10,240 bytes is not displayed in the Guide window.

To use `\` in the message, specify `\\`. To use `$`, specify `\$`. If `$B.`*attribute-name*Δ or `$E.`*attribute-name*Δ is specified in the message, the attribute value corresponding to the JP1 event attribute name is expanded (Δ indicates a space). The monitoring node ID replaces `$T.MONNODEID`Δ (Δ indicates a single-byte space). If there is no corresponding attribute, the attribute is replaced with blanks.

To use a linefeed code in the message, specify `\n`.

`EV_FILE=`*guide-message-file*

Specifies the full path or relative path (from *Scope-path*`\conf\guide\` or `/etc/opt/jp1scope/conf/guide/`) of the file that contains the guide message to be displayed in the Guide window. Note that you can specify this parameter only once between `[EV_GUIDE_`*number*`]` and `[END]`.

Express the file name using a maximum of 1,024 bytes of characters. If the specified file name exceeds 1,024 bytes, an error occurs when JP1/IM - Manager starts or the guide message file is called from JP1/IM - View.

When you specify this parameter, you must specify `2` as the value of `DESC_VERSION`.

The file specified as *guide-message-file* can have any file name and extension. We recommend that you use a file name that is easy to manage, and that you use the extension `.txt` if the guide messages are in TXT format and the extension `.html` or `.htm` if the guide messages are in HTML format.

Examples: `guide001_AJS2.txt`, `guide001_AJS2.htm`

Guide-message file

Specify in the guide-message file in TXT or HTML format the information that you want to display in the Guide window. The information that you can specify is the same as for `EV_GUIDE` in the guide information file. In the case of a guide-message file, you can edit the formatting by inserting linefeed codes.

The contents and syntax of the guide-message file are not checked.

You can store the created guide-message file in any folder. However, when you are operating in a cluster configuration, you should store it in the following folder for purposes of system failover:

- In Windows

shared-folder`\jp1scope\conf\guide\`

- In UNIX

shared-directory`/jp1scope/conf/guide/`

The maximum size of a guide-message file is 1 megabyte. If the file size exceeds 1 megabyte, an error occurs when the guide-message file is loaded from the Guide window of JP1/IM - View.

The table below lists and describes the HTML tags and attributes that can be used to create a guide-message file in HTML format.

Table 2–59: HTML tags that can be used in guide messages

Tag	Attribute	Description
HTML	--	Declares that this is an HTML text. This tag is mandatory.
HEAD	--	Declares the header of the HTML text. This tag is mandatory.
BODY	--	Declares the body of the HTML text. This tag is mandatory.
A	HREF="URL"	Specifies a link-target URL. If a relative path or a URL beginning with `mailto:` is specified, the integrity of the operation is not guaranteed. The link specified here is displayed in the Guide window (HTML format). Clicking the link starts a Web browser and accesses the specified URL.
H1, H2, H3, H4, H5, H6	--	Specifies headers.
FONT	SIZE="*font-size*"	Specifies the font size. The permitted values are from 1 to 7.
	COLOR="*font-color*"	Specifies the font color. You can specify the following 16 colors: `black`, `silver`, `gray`, `white`, `maroon`, `red`, `purple`, `fuchsia`, `green`, `lime`, `olive`, `yellow`, `navy`, `blue`, `teal`, `aqua` If you specify any other font color, the operation is not guaranteed.
B	--	Specifies boldface type.
I	--	Specifies italics type.
HR	--	Specifies an underscore.
BR	--	Specifies a forced linefeed.

Legend:

--: None

If any other HTML tags are used, the integrity of operations is not guaranteed.

`[END]`

Specifies the end tag for the guide information.

Example definition

```
# JP1/IM-CS Guide Information File.

DESC_VERSION=1
[EV_GUIDE_1]
NUM=2
```

```
EV_TITLE=JP1/AJS2  Abnormal termination of job A
EV_COMP_1=T.MONNODEID:0000000A
EV_COMP_2=B.ID:00000111
EV_GUIDE=The job terminated abnormally. \nCheck whether an error has occurre
d on the $E.C0 host.
[END]
[EV_GUIDE_2]
NUM=1
EV_COMP_1=B.ID:00004107
EV_GUIDE=The job terminated abnormally. \nCheck whether an error has occurre
d on the $E.C0 host.\nAs an example of failure, a job failed at host A due t
o a memory shortage in the past. Use the vmstat command to check the availab
le memory capacity.
[END]
```

Settings file for the maximum number of status change events (evhist_warn_event_xxx.conf)

Format

```
[logical-host-name\JP1SCOPE\BMS\EVHISTORY]
"EVHIST_WARN_EVENT"=dword:value
```

File

`evhist_warn_event_on.conf` (used to enable monitoring of the maximum number of status change events)

`evhist_warn_event_off.conf` (used to disable monitoring of the maximum number of status change events)

Storage directory

In Windows

For a physical host:

Scope-path`\conf\`

For a logical host:

shared-folder`\jp1scope\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1scope/conf/`

For a logical host:

shared-directory`/jp1scope/conf/`

Description

This file defines whether a JP1 event is to be issued when the number of status change events exceeds the maximum value (100 events).

When you have enabled this function, a JP1 event is issued when the number of status change events for a monitoring object exceeds 100. The JP1 event that is issued is a warning event whose event ID is `3FB1`.

In JP1/IM - Manager that has been installed as a new installation, this function (issuance of a warning JP1 event) is enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1SCOPE\BMS\EVHISTORY]`

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"EVHIST_WARN_EVENT"=dword:`*value*

- The value of `evhist_warn_event_on.conf` is `00000001` (JP1 event with event ID `3FB1` is issued).
- The value of `evhist_warn_event_off.conf` is `00000000` (JP1 event with event ID `3FB1` is not issued).

Do not edit this parameter.

For details about the JP1 events, see *3.2.2 Details of JP1 events output by JP1/IM - Manager*.

Settings file for the completed-action linkage function (action_complete_xxx.conf)

Format

```
[logical-host-name\JP1SCOPE\BMS]
"ACTION_COMPLETE_MODE"=dword:value
```

File

`action_complete_on.conf` (used to enable the completed-action linkage function)

`action_complete_off.conf` (used to disable the completed-action linkage function)

Storage directory

In Windows

For a physical host:

Scope-path`\conf\`

For a logical host:

shared-folder`\jp1scope\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1scope/conf/`

For a logical host:

shared-directory`/jp1scope/conf/`

Description

This file defines whether the completed-action linkage function is to be enabled.

When the function is enabled, the status of a monitoring object changes on Central Scope according to the JP1 event action status at Central Console.

In JP1/IM - Manager that has been installed as a new installation, this function is enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1SCOPE\BMS]`

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"ACTION_COMPLETE_MODE"=dword:`*value*

- The value of `action_complete_on.conf` is `00000001`.

- The value of `action_complete_off.conf` is `00000000`.

Do not edit this parameter.

Definition file for automatic delete mode of status change event

Format

```
[logical-host-name\JP1SCOPE\BMS\EVHISTORY]
"EVPROCESSED_MODE"=dword:value
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This definition file is used to enable the function that automatically deletes the status change events when a JP1 event's action status becomes **Processed**.

In JP1/IM - Manager that has been installed as a new installation, this function is disabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1SCOPE\BMS\EVHISTORY]`

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"EVPROCESSED_MODE"=dword:`*value*

Specifies `1` to enable the function that automatically deletes status change events and `0` to disable the function.

Definition file for monitoring object initialization mode

Format

```
[logical-host-name\JP1SCOPE\BMS]
"AUTO_INITIALIZE_MODE"=dword:value
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This definition file is used to enable the function that automatically initializes monitoring objects when a specific JP1 event is received.

In JP1/IM - Manager that has been installed as a new installation, this function is disabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1SCOPE\BMS]`

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"AUTO_INITIALIZE_MODE"=dword:`*value*

Specifies `1` to enable the function that automatically initializes monitoring objects and `0` to disable the function.

Automatic backup and recovery settings file for the monitoring object database (auto_dbbackup_xxx.conf)

Format

```
[logical-host-name\JP1SCOPE\BMS]
"AUTO_DB_BACKUP_RECOVERY"=dword:value
```

File

`auto_dbbackup_on.conf` (used to enable the backup and recovery functions for the monitoring object database)

`auto_dbbackup_off.conf` (used to disable the backup and recovery functions for the monitoring object database)

Storage directory

In Windows

For a physical host:

Scope-path`\conf\`

For a logical host:

shared-folder`\jp1scope\conf\`

In UNIX

For a physical host:

`/etc/opt/jp1scope/conf/`

For a logical host:

shared-directory`/jp1scope/conf/`

Description

This file defines whether to enable the function that protects the monitoring object database from corruption that may be caused by OS shutdown or cluster system switching during monitoring tree update processing (automatic backup and recovery functions for the monitoring object database).

If enabled, this function backs up the existing monitoring object database when the monitoring tree is updated, and performs recovery from the backup of the monitoring object database in the event of a failure (if update processing finishes without a failure occurring, the backup data is automatically deleted).

When JP1/IM - Manager is newly installed, this function is enabled by default, but when JP1/IM - Manager is upgraded, the legacy settings are inherited.

When you are operating in a cluster operation system, you must enable this function.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

[*logical-host-name*\JP1SCOPE\BMS]

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify JP1_DEFAULT for the physical host and *logical-host-name* for a logical host.

"AUTO_DB_BACKUP_RECOVERY"=dword:*value*

- The value of auto_dbbackup_on.conf is 00000001.
- The value of auto_dbbackup_off.conf is 00000000.

Do not edit this parameter.

Coding example

This example enables the automatic backup and recovery functions for the monitoring object database of JP1/IM - Manager on the HostA logical host:

```
[HostA\JP1SCOPE\BMS\JCSDB]"AUTO_DB_BACKUP_RECOVERY"=dword:00000001
```

Definition file for object types

Format

```
@encode character-encoding
[comment]
[ObjectType]
definition-block [comment]
[End]
[comment]
```

File

company-name_product-name_company-name_product-name`_obj.en` (definition file for object types)

company-name can be changed to *series-name_product-name*. We recommend that you use the value specified for `PRODUCT_NAME` at the time of JP1 event issuance as the file name, with the forward slash (`/`) replaced by the underscore (_). Because `hitachi` is used for the default file name, use a name other than `hitachi` for *company-name*.

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\object_type\`

For a logical host:

shared-folder`\jp1cons\conf\console\object_type\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/object_type/`

For a logical host:

shared-directory`/jp1cons/conf/console/object_type/`

Description

The definition file for object types defines the object types and root object types that are displayed in **Object type** and **Root object type** in the following JP1/IM - View windows:

- Severe Event Definitions window
- Event Acquisition Settings window
- Common Exclusion-Conditions Settings window
- Common Exclusion-Condition Settings (Extended) window
- Repeated Event Condition Settings window
- Event Search Conditions window
- Settings for View Filter window
- Detailed Settings for Event Receiver Filter window
- Action Parameter Detailed Definitions window

- Severity Change Definition Settings window (Add Severity Change Definition Settings window)
- Display Message Change Definition Settings window (Add Display Message Change Definition Settings window)

For JP1/IM - Manager for Linux, the file must use UTF-8 encoding, and for JP1/IM - Manager for an OS other than Linux, the file must use Shift-JIS or EUC encoding.

If multiple files contain the same object type, the integrity of operations is not guaranteed.

When the definitions are applied

The definition takes effect after JP1/IM - View is restarted.

Information that is specified

`@encode` *character-encoding*

Specifies the character encoding that is to be used in the definition file for object types.

To create an additional file for definition file for object types, use an @encode statement to specify the character set for the definition file.

Item names will be expressed in characters that can be represented in the character encoding specified in the `@encode` statement. In addition, the definition file for object types will be saved in the character encoding specified in the `@encode` statement.

In the following circumstances, item names displayed in JP1/IM - View might be garbled:

- If the item name uses characters that cannot be represented in the character encoding specified in the `@encode` statement
- If the character encoding specified in the `@encode` statement does not match the character encoding in which the file was saved

If no @encode statement exists or if there is an error in the specified character set name that follows the @encode statement, the character set is determined automatically. However, depending on the content of the definition file, the character encoding might not be determined correctly.

The specifiable character encodings are as follows:

- C
- EUCJIS
- SJIS
- UTF-8
- GB18030

Note

If you use UTF-8 as the encoding to save a definition file, save the file without attaching a BOM (byte order mark).

An error is output in the following cases:

- A character encoding other than C, EUCJIS, SJIS UTF-8 or GB18030 is specified
- The definition file does not begin with `@encode`.
- `@encode` is not followed by a character encoding specification.

`[`*comment*`]`

Specifies a comment as a character string that begins with a hash mark (#) and does not contain a linefeed code.

`[ObjectType]`

Specify `[ObjectType]` and `[End]` as is, including the square brackets.

definition-block [*comment*]

A definition block consists of an extended attribute value and a list display character string. The extended attribute value is a character string that is stored in the object type or root object type. The list display character string is a character string that is displayed in a list drop-down list.

`[End]`

Specify `[End]` as is, including the square brackets.

When you define this information, note the following:

- The object type (extended attribute value) cannot contains spaces.
- For list display character strings, specify the extended attribute value itself instead of characters.

Example definition

The following shows an example of a definition file for object types:

```
@encode UTF-8
[ObjectType]
# Extended attribute value,  List display character string   Comment
ACTION,        ACTION          // action
ACTIONFLOW,    ACTIONFLOW      // action flow
BATCHQUEUE,    BATCHQUEUE      // batch queue
JOB,           JOB             // job
JOBNET,        JOBNET          // jobnet
MEDIA,         MEDIA           // media
PRINTER,       PRINTER         // printer
PRINTJOB,      PRINTJOB        // print job
PRINTQUEUE,    PRINTQUEUE      // pipe queue
PROCESS,       PROCESS         // process
RESTORE,       RESTORE         // restore
[End]
```

Definition file for executing applications

Format

```
@file type="definition-file-type", version="definition-format-version";
# comment-line
@define-block type="application-execution-def";
id="application-execution-definition-identifier";
path="command-path";
description="description-of-application-execution";
@define-block-end;
```

File

`!JP1_CC_APP0.conf` (definition file for executing applications)

`!JP1_CC_APP0.conf.model` (model file for the definition file for executing applications)

Storage directory

View-path`\conf\appexecute\en\`

Description

This file defines the IDs and paths of executable files, such as applications that are started from the Event Console window.

JP1/IM provides the `jcoappexecfcheck` command, which checks the contents of the definition file for executing applications. For details about this command, see *jcoappexecfcheck (Windows only)* in *Chapter 1. Commands*.

When the definitions are applied

The definition takes effect after JP1/IM - View is restarted.

Information that is specified

`@file type="application-execution-definition";`

Declares that this is the definition file for executing applications. This statement is mandatory.

This statement must be specified on the first line of the file.

`#` *comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

Application execution definition block

Defines the path of an executable file, such as an application that is started from the Event Console window, and assigns an ID for purposes of linkage from other definition files.

You can specify the following statements in this block:

- `id` statement
- `path` statement
- `description` statement

If any other statement is written, an error is output, and only the applicable statement is ignored.

The following describes the statements.

`id="`*application-execution-definition-identifier*`";`

Specifies an identifier that is to be assigned to the command path that is specified in this block. This statement is mandatory. You can specify this statement only once in a block.

If the file to be analyzed contains multiple blocks with the same `id`, their priority is determined as follows and only the block that has the highest priority is effective:

1. Last block when the file names are sorted in ascending order

2. Last block in the file

All the other blocks are ignored.

The application execution definition identifier is a character string consisting of no more than 32 alphanumeric characters. This character string must be unique within the definition. To achieve uniqueness, observe the following naming convention:

company-name_product-name`[`*_function-name-(or-window-name)*`]`

This cannot be a character string that begins with `jco_` or the character string `default_browser` because they are reserved as application execution definition identifiers.

`path="`*command-path*`";`

Defines the path of the executable file that is to be associated with the application execution definition identifier specified in the `id` statement. This statement is mandatory. You can specify the `path` statement more than once in the same block. Express the executable file that is to be started as a full path. You can also use a substitute keyword discussed below to assemble a path from data such as the registry.

If you specify this statement more than once, the paths are searched in the order specified and the first path found is used.

In the `path` statement, you can specify an `.exe` or `.bat` file as the executable file.

The current directory is undefined during command execution. A command that uses a relative path from the current directory cannot be specified. Execute such a command after you have executed the `cd` command by using a file such as a `.bat` file.

The search processing executes only when JP1/IM - View starts. Therefore, if you have installed an application to be started while JP1/IM - View is running, you must restart JP1/IM - View.

Note that if you attempt to execute a command located under the `%WINDIR%\System32` folder in the 64-bit edition of Windows, the WOW64 redirection function executes the corresponding command under the `%WINDIR%\SysWow64` folder. If the corresponding command does not exist, command execution might fail. Keep this in mind if you specify a path of an executable file under the `%WINDIR%\System32` folder.

Alternate string

In the `path` statement, you can specify an alternate string that can be replaced during execution.

(1) Alternate keyword string

If the specified definition contains an alternate keyword string, the character string is replaced according to the specified keyword. The format is as follows:

`%`*alternate-keyword*`%`

The following table lists the alternate keywords.

Table 2–60: List of alternate keywords

Keyword	Substitute data
`JCO_JP1USER`	JP1 user who logged in to JP1/IM - Manager
`JCO_INSTALL_PATH`	Name of the JP1/IM - View installation folder

(2) Alternate registry string

If the specified definition contains an alternate registry string, the value is acquired from the specified registry to replace the character string. The format of an alternate registry string is as follows:

`[\`*registry-key*`\`*registry-key*`\...\`*registry-value*`]`

In an alternate registry string, you can specify the registry-only substitute keyword `%UPPER%`. If you use `%UPPER%`, the character string for the key name is compared within the same hierarchy in the registry key. The purpose of this keyword is to always acquire the most recent version when the key is classified by the version in the registry key.

You can specify `%UPPER%` only once in a registry string. The following example specifies the registry of JP1/SAMPLE using `%UPPER%`:

```
[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\SAMPLE\%UPPER%\PATHNAME\PATH00]
```

In this example, `%UPPER%` is replaced with the most recent version, so that the most recent executable file is always obtained.

For example, if there are the following two registry keys, the value is acquired from the registry `0700` because `0700` is greater than `0671`:

```
[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\SAMPLE\0671\PATHNAME\PATH00]
[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\SAMPLE\0700\PATHNAME\PATH00]
```

`description="`*description-of-application-execution*`";`

Adds a description to the application execution definition in the block. You can specify this statement only once in a block.

There is no limit to the number of characters, but we recommend that you specify no more than 50 characters.

The following shows an example of an application execution definition block:

```
@define-block type="application-execution-def";
id="HITACHI_JP1_SAMPLE";
path="C:\Program Files\Hitachi\JP1\bin\sample.exe";
description="Hitachi Sample Program";
@define-block-end;
```

Example definition

The following shows an example of a definition file for executing applications:

```
@file type="application-execution-definition", version="0300";
#------------------------------------------
@define-block type="application-execution-def";
id="jco_notepad";
path="C:\winnt40\system32\notepad.exe";
@define-block-end;
#------------------------------------------
@define-block type="application-execution-def";
id="jco_dmp";
path="[\HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P\0521/
    A\PathName\Path00]\bin\DMPSTS.exe";
@define-block-end;
```

Definition file for on memory mode of status change condition

Format

```
[logical-host-name\JP1SCOPE\BMS]
"EVENT_MATCH_MODE"=dword:value
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This definition file is used to enable the memory-resident status change condition function.

In JP1/IM - Manager that has been installed as a new installation, this function is enabled. In JP1/IM - Manager that has been installed as an upgrade installation, the same setting that was specified in the previous version is initially retained.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted by executing the `jbssetcnf` command.

Information that is specified

`[`*logical-host-name*`\JP1SCOPE\BMS]`

Specifies the key name for the JP1/IM environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for the physical host and *logical-host-name* for a logical host.

`"EVENT_MATCH_MODE"=dword:`*value*

To enable the memory-resident status change condition function, specify `1`; to disable the function, specify `0`.

Severity changing definition file (jcochsev.conf)

Format

```
DESC_VERSION=version-information

def definition-name-1
    [cmt comment]
    [define {enable | disable}]
    [addflag {true | false}]
    cnd
        event-condition
    end-cnd
    sev event-level
end-def

def definition-name-2
    [cmt comment]
    [define {enable | disable}]
    [addflag {true | false}]
    cnd
        event-condition
    end-cnd
    sev event-level
end-def
```

File

`jcochsev.conf` (severity changing definition file)

`jcochsev.conf.model` (model file for the severity changing definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chsev\`

For a logical host:

shared-folder`\jp1cons\conf\chsev\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chsev/`

For a logical host:

shared-directory`/jp1cons/conf/chsev/`

Description

This file defines conditions for changing the event level of JP1 events and the new event level. The event severity changing function changes the event level of a JP1 event if it satisfies an event condition defined in this file. Specify this file using the language encoding that is used by JP1/IM - Manager.

The maximum size of this file is 17 megabytes (17,825,792 bytes). There is no upper limit on the number of definitions.

There are two types of parameters in the severity changing definition file:

- Severity changing definition file version
  Defines the format version of the severity changing definition file.
- Severity changing definition parameter
  Defines a condition for JP1 events whose event level is to be changed and the new event level. The higher a severity changing definition is listed in the severity changing definition file, the higher its priority.

When the definitions are applied

The definition takes effect when the event severity changing function is enabled, and one of the following operations is performed:

- JP1/IM - Manager is started.
- The `jco_spmd_reload` command is executed.
- The **OK** button is clicked in the Add Severity Change Definition Settings window.
- The **Apply** button is clicked in the View Severity Change Definitions window.

Information that is specified (severity changing definition file version)

`DESC_VERSION`

Specifies the file version that determines the format of this severity changing definition file as version information. Specify `2`. If `DESC_VERSION` is omitted, `2` is assumed as the file version.

Specify `DESC_VERSION` on the first line of the definition file (the first line in the file excluding any null lines and comment lines). If there is no file version in the first line, `2` is assumed.

Table 2–61: Version information of the severity changing definition file format

Version information	Description
`1`	Indicates version 10-10 or earlier as the version of the severity changing definition file.
`2`	Indicates version 10-50 as the version of the severity changing definition file.

Table 2–62: List of parameters that can be specified in the severity changing definition file according to the version information

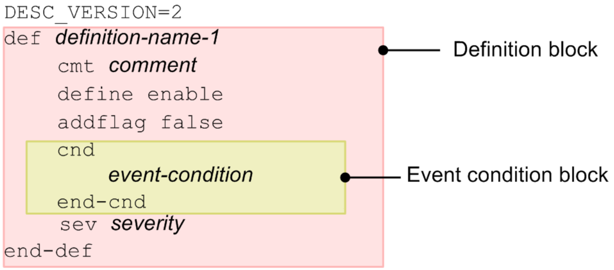
Version information	Parameter name
1	`def` to `end-def` (definition block) `cnd` to `end-cnd` (event condition block) `sev`

2	`def` to `end-def` (definition block)
	`cmt` *comment*
	`define {enable | disable}`
	`addflag {true | false}`
	`cnd` to `end-cnd` (event condition block)
	`sev`

Information that is specified (severity changing definition parameter)

As shown in the following figure, the definition parameter for changing severity consists of a definition block and an event condition block.

Figure 2–9: Parameter for changing severity



```
DESC_VERSION=2
def definition-name-1
    cmt comment
    define enable
    addflag false
    cnd
        event-condition
    end-cnd
    sev severity
end-def
```

`def` to `end-def` (definition block)

These are the start and end parameters for a severity changing definition. The block from `def` to `end-def` can be omitted, in which case the system assumes that the event level is not to be changed for any JP1 events. After `def`, specify the names of severity changing definitions. If you specify `def`△△△*definition-1*△△△*definition-2*△△△, then △△*definition-1*△△△*definition-2*△△△ are treated as the definition names (Δ indicates a single-byte space).

For a definition name, specify a character string of from 1 to 50 bytes. Each definition name must be unique within the severity changing definition file. The permitted characters are all characters other than the control characters (from `0x00` to `0x1F` and `0x7F` to `0x9F`).

`cmt` *comment*

Describes the comment for the severity changing definition. The comment specified for `cmt` is displayed in the comment section of the Severity Change Definition Settings window. Only one `cmt` parameter can be specified in the definition block. This parameter can be omitted. Specify the comment within 1,024 bytes. The permitted characters are all characters other than the control characters (`0x00` to `0x1F`, and `0x7F` to `0x9F`).

If you specify this parameter when *version-information* is 1, an error occurs.

`define {enable | disable}`

Specifies whether to enable the severity changing definition. Only one `define` parameter can be specified in the definition block. To enable the severity changing definition, specify `enable`, to disable it, specify `disable`. The `define` parameter can be omitted. By default, `enable` is set. The values are not case sensitive.

If you specify this parameter when *version-information* is 1, an error occurs.

`addflag {true | false}`

Indicates an additional severity changing definition has been added from a window, and specifies whether the severity changing definition is an additional severity changing definition. Therefore, to edit the severity changing definition file, you do not need to specify the `addflag` parameter. Only one `addflag` parameter can be specified in the definition block. Specify `true` for the additional severity changing definition, and `false` for the severity changing definition. When `true` is specified, the icon (📎) is displayed in **Type** of the View Severity Change Definitions window. The `addflag` parameter can be omitted. By default, `false` is specified. The value is not case sensitive.

If you specify this parameter when *version-information* is 1, an error occurs.

`cnd` to `end-cnd` (event condition block)

These are the start and end parameters for the block that specifies a condition for the JP1 events whose event level is to be changed. You must specify one event condition block in a definition block. The event condition block cannot be omitted. If a received JP1 event satisfies multiple event conditions, the definition block closest to the beginning of the severity changing definition file is effective. Tabs and spaces before and after the `cnd` and `end-cnd` parameters are ignored.

event-condition

Specifies a condition for the JP1 events whose event level is to be changed. You can specify from 0 to 256 event conditions in an event condition block. You can specify from 1 to 256 event conditions per event condition block. When multiple event conditions are specified, it is assumed that they are connected with the AND condition. Specify the event conditions in the following format (Δ indicates a single-byte space):

*attribute-name*Δ*comparison-keyword*Δ*operand* [Δ*operand*] ...

Note that a line consisting of only spaces or tabs is ignored during processing.

attribute-name

Specifies the name of the attribute that you want to compare. To specify a basic attribute, place `B.` immediately before the name. To specify an extended attribute (common information or user-specific information), place `E.` immediately before the name. The attribute names are case sensitive.

The following table lists and describes the combinations of attribute names and comparison keywords and the operands that can be specified.

Table 2–63: Combinations of attribute names and comparison keywords and the operands that can be specified

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	`B.ID`	• `Match` • `Does not match`	A maximum of 100 event IDs can be specified. Specify event IDs in hexadecimal notation. Event IDs are not case sensitive. The permitted range is from `0` to `7FFFFFFF`.
2	Reason for registration	`B.REASON`	• `Match` • `Does not match`	A maximum of 100 reasons for registration can be specified.
3	Source process ID	`B.PROCESSID`	• `Match` • `Does not match`	A maximum of 100 source process IDs can be specified. The permitted value range is from -2,147,483,648 to 2,147,483,647.
4	Source user ID	`B.USERID`	• `Match` • `Does not match`	A maximum of 100 source user IDs can be specified. The permitted value range is from -2,147,483,648 to 2,147,483,647.
5	Source group ID	`B.GROUPID`	• `Match` • `Does not match`	A maximum of 100 source group IDs can be specified. The permitted value range is from -2,147,483,648 to 2,147,483,647.
6	Source user name	`B.USERNAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 source user names can be specified. However, if a regular expression is used, only one source user name is allowed.
7	Source group name	`B.GROUPNAME`	• `First characters` • `Match`	A maximum of 100 source group names can be specified. However, if a regular expression is used, only one source group name is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	
8	Event-issuing server name (source host)#1	`B.SOURCESERVER`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 event-issuing server names can be specified. However, if a regular expression is used, only one event-issuing server name is allowed.
9	Target event server name#1	`B.DESTSERVER`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 target event server names can be specified. However, if a regular expression is used, only one target event server name is allowed.
10	Message	`B.MESSAGE`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 messages can be specified. However, if a regular expression is used, only one message is allowed.
11	Severity	`E.SEVERITY`	• `Match`	Multiple severity values can be specified. However, if a regular expression is used, only one severity value is allowed. The following are the specifiable values: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, or `Debug`.
12	User name	`E.USER_NAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 user names can be specified. However, if a regular expression is used, only one user name is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
13	Product name	`E.PRODUCT_NAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 product names can be specified. However, if a regular expression is used, only one product name is allowed.
14	Object type	`E.OBJECT_TYPE`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 object types can be specified. However, if a regular expression is used, only one object type is allowed.
15	Object name	`E.OBJECT_NAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 object names can be specified. However, if a regular expression is used, only one object name is allowed.
16	Root object type	`E.ROOT_OBJECT_TYPE`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 root object types can be specified. However, if a regular expression is used, only one root object type is allowed.
17	Root object name	`E.ROOT_OBJECT_NAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 root object names can be specified. However, if a regular expression is used, only one root object name is allowed.
18	Object ID	`E.OBJECT_ID`	• `First characters` • `Match` • `Does not match` • `Is contained`	A maximum of 100 object IDs can be specified. However, if a regular expression is used, only one object ID is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• `Is not contained` • `Regular expression`	
19	Occurrence	`E.OCCURRENCE`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 occurrences can be specified. However, if a regular expression is used, only one occurrence is allowed.
20	Result code	`E.RESULT_CODE`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 termination codes can be specified. However, if a regular expression is used, only one termination code is allowed.
21	Event source host name[#1]	`E.JP1_SOURCEHOST`	• `First characters` • `Match` • `Do not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 event source host names can be specified. However, if a regular expression is used, only one event source host name is allowed.
22	Program-specific extended attribute[#2]	`E.`*xxxxxxx*	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	For the attribute name, you can specify a name with a maximum length of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_). A maximum of 100 extended attributes can be specified. However, if a regular expression is used, only one extended attribute is allowed.

#1

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is `Match` or `Do not match`, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than `Match` and `Do not match` is selected, a business group name specified in a path format is treated as a host name.

If the `-ignorecasehost` option of the `jcoimdef` command is set to `ON`, and a comparison keyword other than `Regular expression` is selected, the character string is no longer case sensitive.

#2

You can also specify a JP1 product-specific extended attribute. For example, the program-specific extended attribute for the JP1/AJS job execution host is `E.C0`. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

•*comparison-keyword*

Specifies one of BEGIN (begins with), IN (matches), NOTIN (does not match), SUBSTR (includes), NOTSUBSTR (does not include), or REGEX (regular expression) as the comparison keyword. The comparison keyword is case sensitive.

•*operand*

Specifies a character string as the value that is to be compared with the attribute value by the specified comparison keyword. Operands are case sensitive.

Separate multiple operands with one or more consecutive spaces or a tab. The OR condition is applied to the specified operands. Note that if a regular expression is specified, only one operand can be specified.

To specify a space, a tab, end-of-line code (CR or LF), or % as part of an operand, specify as follows:

No.	Value to be set	How to specify
1	Tab (0x09)	%09
2	Space (0x20)	%20
3	% (0x25)	%25
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.IDΔINΔ100Δ200

Legend:

Δ: Space (0x20)

You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length in bytes of all operands that are specified in the event condition block).

sev

Specifies the new event level after the change.

You must specify one sev parameter in a definition block. This parameter cannot be omitted.

You can specify in the sev parameter Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug.

#*comment-line*

A line beginning with a hash mark (#) is treated as a comment. Note that if you set the severity changing definition from JP1/IM - View, the comment line beginning with # is deleted.

Example definition

Change the event level to Emergency when the event ID is 100 or 200, the existing event level is Warning, and the source host is hostA, hostB, or hostC:

```
DESC_VERSION=2
def Event level change 1
    cmt comment1
    define enable
    cnd
        B.ID IN 100 200
        E.SEVERITY IN Warning
        B.SOURCESERVER IN hostA hostB hostC
    end-cnd
    sev Emergency
end-def
```

Display item definition file for the severity change definition (chsev_attr_list.conf)

Format

```
# comment-line
attribute-name
attribute-name
   .
   .
attribute-name
```

File

`chsev_attr_list.conf` (display item definition file for the severity change definition)

`chsev_attr_list.conf.model` (model file of the display item definition file for the severity change definition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chsev\attr_list`

For a logical host:

shared-folder`\jp1cons\conf\chsev\attr_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chsev/attr_list`

For a logical host:

shared-directory`/jp1cons/conf/chsev/attr_list`

Description

This definition file specifies the items to display in the Attribute name display area of the Severity Change Definition Settings window. The display items specified in the display item definition file for the severity change definition are displayed in the Attribute name display area of the Severity Change Definition Settings window in the specified order.

When the definitions are applied

The contents of the definition file take effect when Central Console is started, and the definition is reloaded by executing the `jco_spmd_reload` command.

Information that is specified

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

attribute-name

For the display item definition file for the severity change definition, specify the display items to display in the **Attribute name** display area of the Severity Change Definition Settings window. Write an attribute name corresponding to the display item per line. You can specify 0 to 256 display items.

The attribute name is case sensitive. Single-byte spaces and tabs before or after the attribute name are ignored.

If you specify `SEPARATOR`, `--------------------` is displayed in the **Attribute name** display area of the Severity Change Definition Settings window. You can set `SEPARATOR` to separate frequently used items from those used less frequently.

However, if you specify only `SEPARATOR`, only `--------------------` is displayed in the **Attribute name** display area. In this case, if you select `--------------------`, you cannot set the attribute name.

The following table lists the specifiable attribute names.

Table 2–64: List of display items

No.	Display item	Attribute name
1	Event source host name[#]	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`
10	Message	`B.MESSAGE`
11	Product name	`E.PRODUCT_NAME`
12	Event ID	`B.ID`
13	Destination event server name	`B.DESTSERVER`
14	Program-specific extended attribute	`OTHER_EXTENDED_ATTRIBUTE`
15	Reason for registration	`B.REASON`
16	Source process ID	`B.PROCESSID`
17	Source user name	`B.USERNAME`
18	Source user ID	`B.USERID`
19	Source group name	`B.GROUPNAME`
20	Source group ID	`B.GROUPID`
21	Object ID	`E.OBJECT_ID`
22	Result code	`E.RESULT_CODE`
23	--------------------	`SEPARATOR`

Note:

If the same attribute name is specified twice, both specifications are ignored.

Also, if the display item definition file for the severity change definition cannot be read, and the number of valid display items is 0, items 1 to 22 are displayed.

#

If the mapping function of the source host is not enabled, the event source host name is not displayed in the Severity Change Definition Settings window.

Auto-input definition file for the severity change definition (chsev_auto_list.conf)

Format

```
# comment-line
[DEFAULT_NAME severity-changing-definition-name]
attribute-name
attribute-name
   .
   .
attribute-name
attribute-name
```

File

`chsev_auto_list.conf`

`chsev_auto_list.conf.model` (model file of the auto-input definition file for the severity change definition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chsev\auto_list`

For a logical host:

shared-folder`\jp1cons\conf\chsev\auto_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chsev/auto_list`

For a logical host:

shared-directory`/jp1cons/conf/chsev/auto_list`

Description

This file defines the JP1 event attribute that is set automatically when you select a JP1 event in the event list of the Event Console window, select **View**, and then **Add Severity Change Definition Settings** to open the Add Severity Change Definition Settings window. Also, the default severity changing definition name can be defined.

When the definitions are applied

The contents of the definition file take effect when Central Console starts, and when the definition is reloaded by executing the `jco_spmd_reload` command.

Information that is specified

`#` *comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

`DEFAULT_NAME` *severity-changing-definition-name*

Indicates the identifier that defines the severity changing definition name. The identifier must be written at the beginning of the file excluding the comment and blank lines.

The severity changing definition name specified for this parameter is displayed as the initial value when you select a JP1 event from the event list in the Event Console window, select **View**, and then **Add Severity Change Definition Settings** to open the Add Severity Change Definition Settings window.

Specify a character string of maximum of 40 bytes. Any characters, other than control characters (`0x00` to `0x1F`, and `0x7F` to `0x9F`), are permitted. If you specify over 40 bytes of characters, the characters from the 41st byte are dropped, and the first 40 bytes are treated as the severity changing definition name. If you omit this parameter, *additional-severity-changing-definition* is used as the *severity-changing-definition-name*.

attribute-name

For the auto-input definition file for the severity change definition, specify the JP1 event attribute which is set as an event condition when you select a JP1 event from the event list in the Event Console window, select **View**, and then **Add Severity Change Definition Settings** to open the Add Severity Change Definition Settings window. The attribute name condition specified for this parameter is displayed as the initial value when you select a JP1 event from the event list in the Event Console window, select **View**, and then **Add Severity Change Definition Settings** to open the Add Severity Change Definition Settings window.

For the definition item, specify one attribute name of the JP1 event to be set for each line.

The attribute name is case sensitive. Single-byte spaces or tabs before or after the attribute name are ignored.

Note that if you specify the same attribute name more than once, both values are ignored, and the `KAVB1935-W` message is output to the integrated trace log file.

JP1 event attributes are displayed automatically in the **Event conditions** section of the Severity Change Definition Settings window in the order they were written in the display item definition file for the severity change definition (`chsev_attr_list.conf`).

The following table lists the specifiable attribute names.

Table 2–65: List of display items

No.	Display item	Attribute name
1	Event source host name#	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`
10	Message	`B.MESSAGE`
11	Product name	`E.PRODUCT_NAME`
12	Event ID	`B.ID`
13	Destination event server name	`B.DESTSERVER`
14	Reason for registration	`B.REASON`
15	Source process ID	`B.PROCESSID`

No.	Display item	Attribute name
16	Source user name	B.USERNAME
17	Source user ID	B.USERID
18	Source group name	B.GROUPNAME
19	Source group ID	B.GROUPID
20	Object ID	E.OBJECT_ID
21	Result code	E.RESULT_CODE

Note:

If the same attribute name is specified twice, both specifications are ignored.

Also, if the auto-input definition file for the severity change definition cannot be read, and the number of valid display items is 0, items 1 to 3, and items 10 to 12 are displayed.

#

If the mapping function of the source host is not enabled, the event source host name is not displayed in the Add Severity Change Definition Settings window.

Communication environment definition file (view.conf.update)

Format

```
[JP1_DEFAULT\JP1CONSOLEVIEW]
"COM_SO_TIMEOUT"=dword:hexadecimal-value
"COM_RMI_TIMEOUT"=dword:hexadecimal-value
```

File

`view.conf.update` (model file for the communication environment definition file)

Storage directory

View-path`\default\`

Description

This file defines timeout periods for communication between JP1/IM - View and JP1/IM - Manager (Central Console).

When a low-speed line is used in the network or when the viewer's workload is high, timeouts might occur during the viewer's communication processing, resulting in communication errors. You can prevent such communication errors by modifying timeout periods. If you set a timeout period, you must also specify the same setting at the JP1/IM - Manager (Central Console) that is connected.

If you change any value in this definition file, you must also change the value in the communication environment definition file for JP1/IM - Manager (Central Console).

The required definition is provided as a model file. To change the settings, copy the model file and then edit the copy.

When the definitions are applied

The definitions take effect after the `jbssetcnf` command is executed and JP1/IM - View is restarted.

Information that is specified

`[JP1_DEFAULT\JP1CONSOLEVIEW]`

Specifies the key name for the JP1/IM - View environment settings.

In JP1/IM - View, this parameter is fixed.

`"COM_SO_TIMEOUT"=dword:`*hexadecimal-value*

Specify in milliseconds as a hexadecimal value the amount of time to wait for the arrival of reception data (socket timeout value). The default value is `dword:0000EA60` (60,000 milliseconds).

In an environment in which a low-speed line is used or event traffic is heavy, specify a larger value.

The range of values that can be specified is `0x00000001` to `0x0036EE80` (3,600,000 milliseconds).

The specified value must not exceed the value specified for `COM_RMI_TIMEOUT` (default: `0000EA60`) in the `view.conf.update` communication environment definition file.

`"COM_RMI_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the timeout period for communication processing during the following operations or settings:

- Login

- Logout
- Manual and automatic refreshing of the Event Console window
- Changing the event action status
- Deletion of server events
- Event search
- User environment setting
- Severe event setting
- Automated action setting
- Filter setting
- Command execution
- Function status notification recovery operation
- Response to a response-waiting event and release from the hold-and-accumulate state

The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0000EA60` (60,000 milliseconds).

Example

```
[JP1_DEFAULT\JP1CONSOLEVIEW]
"COM_SO_TIMEOUT"=dword:000009C4
"COM_RMI_TIMEOUT"=dword:0000EA60
```

Communication environment definition file (tree_view.conf.update)

Format

```
[JP1_DEFAULT\JP1CONSOLEVIEW]
"SOV_LOGIN_TIMEOUT"=dword:hexadecimal-value
"SOV_GETTREE_TIMEOUT"=dword:hexadecimal-value
"SOV_SETTREE_TIMEOUT"=dword:hexadecimal-value
"SOV_MAKETREE_TIMEOUT"=dword:hexadecimal-value
"SOV_GETMAP_TIMEOUT"=dword:hexadecimal-value
"SOV_SETMAP_TIMEOUT"=dword:hexadecimal-value
"SOV_GETPROFILE_TIMEOUT"=dword:hexadecimal-value
"SOV_SETPROFILE_TIMEOUT"=dword:hexadecimal-value
"SOV_DEF_TIMEOUT"=dword:hexadecimal-value
```

File

`tree_view.conf.update` (model file for the communication environment definition file)

Storage directory

View-path`\default\`

Description

This file defines timeout periods for communication between JP1/IM - View and JP1/IM - Manager (Central Scope).

When a low-speed line is used in the network or when the viewer's workload is high, timeouts might occur during the viewer's communication processing, resulting in communication errors. You can prevent such communication errors by modifying timeout periods.

The required definition is provided as a model file. To change the settings, copy the model file and then edit the copy.

When the definitions are applied

The definition takes effect after the `jbssetcnf` command is executed and JP1/IM - View is restarted.

Information that is specified

`[JP1_DEFAULT\JP1CONSOLEVIEW]`

Specifies the key name for the JP1/IM - View environment settings.

In JP1/IM - View, this parameter is fixed.

`"SOV_LOGIN_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for login and logout processing. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0002BF20` (180,000 milliseconds).

`"SOV_GETTREE_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for acquisition of the status of monitoring objects, updating of the monitoring tree, and performance of display processing for the Monitoring Tree (Editing) window. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0036EE80` (3,600,000 milliseconds).

`"SOV_SETTREE_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for changing of the status of monitoring objects, setting of monitoring targets, and performance of tree update processing. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0036EE80` (3,600,000 milliseconds).

`"SOV_MAKETREE_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for performance of automatic generation of the monitoring tree. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0036EE80` (3,600,000 milliseconds).

`"SOV_GETMAP_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for performance of display processing for the visual monitoring list and for the Visual Monitoring window. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0002BF20` (180,000 milliseconds).

`"SOV_SETMAP_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for creation, deletion, and copying of visual monitoring maps, and for performance of visual monitoring update processing. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0002BF20` (180,000 milliseconds).

`"SOV_GETPROFILE_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for acquisition of user environment settings and system environment settings for the Monitoring Tree window. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0002BF20` (180,000 milliseconds).

`"SOV_SETPROFILE_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for performance of reflection processing of user environment settings and system environment settings for the Monitoring Tree window. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:0002BF20` (180,000 milliseconds).

`"SOV_DEF_TIMEOUT"=dword:`*hexadecimal-value*

Specifies in milliseconds as a hexadecimal value the server response wait time for acquisition and setting of monitoring object properties, acquisition of a list of login users, and acquisition of automatically generated configuration selections. The permitted value range is from `0000EA60` to `0036EE80` (from 60,000 to 3,600,000 milliseconds), and the default is `dword:001B7740` (1,800,000 milliseconds).

Example definition

```
[JP1_DEFAULT\JP1CONSOLEVIEW]
"SOV_LOGIN_TIMEOUT"=dword:0002BF20
"SOV_GETTREE_TIMEOUT"=dword:0002BF20
"SOV_SETTREE_TIMEOUT"=dword:0002BF20
"SOV_MAKETREE_TIMEOUT"=dword:0036EE80
"SOV_GETMAP_TIMEOUT"=dword:0002BF20
"SOV_SETMAP_TIMEOUT"=dword:0002BF20
"SOV_GETPROFILE_TIMEOUT"=dword:0002BF20
"SOV_SETPROFILE_TIMEOUT"=dword:0002BF20
"SOV_DEF_TIMEOUT"=dword:0002BF20
```

Non-encryption communication host configuration file (nosslhost.conf)

Format

```
[NO_SSL_HOST]
manager-host-name
manager-host-name
     :
manager-host-name
```

File

`nosslhost.conf` (non-encryption communication host configuration file)

`nosslhost.conf.model` (model file for the non-encryption communication host configuration file)

Storage directory

View-path`\conf\ssl`

Description

This file is for configuring which hosts are to use non-encrypted communication. By default, this file specifies non-encrypted communication for all hosts, so if you want to use encrypted communication, you must configure this file. If you want JP1/IM - View to use non-encrypted communications upon login to a manager host, you must define the host in this file. Communication with manager hosts that are not defined in this file will be encrypted.

JP1/IM - View compares the destination host name in the Login window and the connection target host name specified in the `-h` option of the `jcoview` or `jcfview` command against the manager host names listed in the definition file, and if there is a match, uses non-encrypted communication with the host. The host names are not case sensitive.

When the definitions are applied

The settings for the non-encryption communication host configuration file take effect at the following times:

- When you log in to Central Console from the Central Console viewer, log in to Central Scope from the Central Scope viewer, or log in to IM Configuration Management from the IM Configuration Management viewer (when you display the Login window and click the **OK** button to log in)
- When you display the Central Console viewer or Central Scope viewer from the IM Configuration Management viewer
- When you display the site manager's IM Configuration Management viewer from the IM Configuration Management viewer (Launch Base View)

The following table shows whether the non-encryption communication host configuration file is read when different viewers are launched

Table 2–66: Whether the non-encryption communication host configuration file is read when different viewers are launched

Calling window (operation in calling window)	Check box		Viewer to be launched	Definition file is read
	Central Console	Central Scope		
Login window of the Central Console viewer or Central Scope viewer (click **OK** button)	C	U	Central Console	Y
	U	C	Central Scope	Y
	C	C	Central Console and Central Scope	Y#
Login window of the IM Configuration Management viewer (click **OK** button)			IM Configuration Management	Y
Login window of the Central Scope viewer (click **OK** button) Launch from Monitoring Tree (Editing) window			Central Scope	Y
Central Console viewer (Main menu or toolbar)			Central Scope	N
Central Scope viewer (Main menu or toolbar)			Central Console	N
IM Configuration Management viewer (Main menu or toolbar)			Central Console	Y
			Central Scope	Y
IM Configuration Management viewer (Launch Base View)			Site manager's IM Configuration Management	Y

Legend:

Y: The definition file is read.

N: The definition file is not read.

C: The check box is selected.

U: The check box is not selected.

#

Although two viewers (the Central Console viewer and Central Scope viewer) are launched, the definition file is only read once.

Information that is specified

`[NO_SSL_HOST]`

This block is mandatory. Uppercase and lowercase are distinguished. Any space or tab character immediately preceding or following `[NO_SSL_HOST]` will be ignored.

manager-host-name

Specify the host name or IPv4 address of a destination manager host for which non-encrypted communication is to be used. You can also specify *manager-host-name* in FQDN format. By default, an asterisk (`*`) is set. The wildcard asterisk (`*`) indicates that non-encrypted communication is to be used for connections to all manager hosts. A maximum of 1,024 hosts can be listed. You cannot list the same manager host name more than once. Letter case is ignored. Specify between 0 and 255 characters. Any space or tab character immediately preceding or following *manager-host-name* will be ignored.

Example definition

Example definition 1: Use non-encrypted communication to communicate with all manager hosts

```
[NO_SSL_HOST]
*
```

Specifying an asterisk (*) indicates that non-encrypted communication to is to be used with all manager hosts. When an asterisk (*) is specified, an error results if anything other than the above is specified.

Example definition 2: Use encrypted communication to communicate with all manager hosts

```
[NO_SSL_HOST]
```

To use encrypted communication to communicate with all manager hosts, delete the asterisk (*).

Example definition 3: Use a mixture of non-encrypted and encrypted communication to communicate with manager hosts

```
[NO_SSL_HOST]
hostA
hostB
```

Communication with the manager hosts `hostA` and `hostB` will be non-encrypted, while communication with other manager hosts will be encrypted.

IM-View settings file (tuning.conf)

Format

```
LOGIN_HISTORY_MAX=number-of-connected-host-log-entries
MENU_AUTO_START={ON | OFF}
ACTIONLIST_AUTO_START={ON | OFF}
WWW_BROWSER_PATH=start-path-of-browser
CLIPBOARD_OUTPUT={ON | OFF}
LOGIN_USER_HISTORY_MAX={0|1}
SCREEN_TITLE_LOGININFO={ON | OFF}
```

File

`tuning.conf` (IM-View settings file)

`tuning.conf.model` (model file for the IM-View settings file)

Storage directory

View-path`\conf\`

Description

This file defines the operation of JP1/IM - View, such as the number of connected-host log entries in the Login window, the operation when the Event Console window is displayed, and whether data can be copied to the clipboard.

Specify each item in the `tuning.conf` file in the format *parameter-name*=*value*. The following lines are ignored in the definition file:

- A line consisting only of spaces
- A line beginning with a hash mark (`#`) or a hash mark preceded by any number of spaces (comment line)

When the definitions are applied

The definition takes effect after JP1/IM - View is restarted.

Information that is specified

`LOGIN_HISTORY_MAX=`*number-of-connected-host-log-entries*

Specifies the number of entries (hosts to which connection has been made) that are to be displayed in the **Host to connect** list box in the login window.

The permitted value range is from 0 to 20. If `0` is specified, no history of connected hosts is displayed. If this parameter is omitted, `5` is assumed. The default is `5`.

`MENU_AUTO_START={ON | OFF}`

Specifies whether the Tool Launcher is to be started when the Event Console window is displayed. If you specify `ON`, the Tool Launcher window is opened when the Event Console window is displayed. If you specify `OFF`, the Tool Launcher window is not opened when the Event Console window is displayed. If this parameter is omitted, `OFF` is assumed. The default is `OFF`.

`ACTIONLIST_AUTO_START={ON | OFF}`

Specifies whether the List of Action Results window is to be displayed when the Event Console window is displayed. If you specify `ON`, the List of Action Results window is opened when the Event Console window is displayed. If you specify `OFF`, the List of Action Results window is not opened when the Event Console window is displayed. If this parameter is omitted, `OFF` is assumed. The default is `OFF`.

`WWW_BROWSER_PATH=`*start-path-of-browser*

Specifies the start path of the Web browser that is to be used to open the Tool Launcher and monitor windows. The default is that this parameter is not specified. If you specify this parameter, you must add a parameter in the definition file.

When you specify a path, express \ as \\. Do not enclose the start path name in double-quotation marks ("). Make sure that the specified Web browser is supported by the Tool Launcher and the application that is started when monitor windows are opened.

If this parameter is omitted, the Web browser associated with files of the `.html` file type on the host is used. Specify this parameter in order to use a Web browser that is not associated with files of the `.html` file type (including a different version of the same Web browser).

`CLIPBOARD_OUTPUT={ON | OFF}`

Specifies whether the function for copying JP1 event information, action results, and command execution results to the clipboard is to be enabled.

Specifying `ON` enables the function for copying to the clipboard. When it is enabled, you use this function by selecting the information in the JP1/IM - View window that you want to copy, and then pressing the **Ctrl** and **C** keys to copy it in CSV format to the clipboard. In the Event Console window, **Copy** is displayed in the **Edit** menu.

Specifying `OFF` disables the function for copying to the clipboard.

If this parameter is omitted, `ON` is assumed.

`LOGIN_USER_HISTORY_MAX={0|1}`

Specifies whether to display the names of JP1 users who have logged in previously in the **User name** text box of the Login window. When `1` is specified, the names of users who logged in previously are displayed. When `0` is specified, the names are hidden. If you omit this parameter, or if you specify a value other than `0` or `1`, `1` is assumed. The default is `1`.

`SCREEN_TITLE_LOGININFO={ON | OFF}`

You can prevent the name of the logged-in JP1 user from being displayed in the title of the Monitoring Tree window, the Monitoring Tree (Editing) window, the Visual Monitoring (Editing) window, the Event Console window, the Execute Command window, and the List of Action Results window. The `ON` specification displays the name of the logged-in JP1 user. The `OFF` specification hides name of the logged-in JP1 user. The default is `ON`. If you omit this parameter, or if you specify a value other than `ON` or `OFF`, `ON` is assumed. The value is case sensitive.

Example definition

```
# **********************************************************
# * JP1/Integrated Management - View   Tuning definition file *
# **********************************************************

# Input history maximum number in connected hostname input field on log in s
creen
LOGIN_HISTORY_MAX=5
# Tool Launcher is automatically started at log in whether (ON) (OFF).
MENU_AUTO_START=OFF
# List of Action Result is automatically started at log in whether (ON) (OFF
).
  ACTIONLIST_AUTO_START=OFFCLIPBOARD_OUTPUT=ON
# Copies JP1 event information, action results, and command execution result
s to the clipboard (ON) (OFF).
CLIPBOARD_OUTPUT=ON
# Displays the names of previously logged-in users in the Login window (1) (
0).
LOGIN_USER_HISTORY_MAX=1
# Displays the user name in the window title bar (ON) (OFF).
SCREEN_TITLE_LOGININFO=ON
```

Definition file for opening monitor windows

Format

```
[@encode character-encoding]
DESC_VERSION=0300
{key-definition(SUBKEY parameter is used)
subkey-definition
association-definition
|key-definition(INTERFACE parameter is used)}
call-interface-definition
```

File

hitachi_xxxx`_mon.conf`

(definition file for opening monitor windows for a linked product)

company-name_product-name`_mon.conf`

(user-defined definition file for opening monitor windows)

company-name_series-name_product-name`_mon.conf`

(user-defined definition file for opening monitor windows)

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\monitor\`

For a logical host:

shared-folder`\jp1cons\conf\console\monitor\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/monitor/`

For a logical host:

shared-directory`/jp1cons/conf/console/monitor/`

Description

This definition file is used to define settings for calling monitor windows (such as a monitor window at an event source) from the Integrated Operation Viewer window of Intelligent Integrated Management Base, or the Event Console window of Central Console. Use this file to create a key from information such as the event ID and attributes, and a command line parameter from the event attributes.

The encoding defined in the definition file for calling monitor windows must be UTF-8 for JP1/IM - Manager for Linux and Shift-JIS or EUCJIS for JP1/IM - Manager for an OS other than Linux. Because, hitachi is used for the default file name, use a name other than *hitachi* for *company-name*.

If *hitachi* is specified for the company name in a definition file for opening monitor windows, this definition file contains system standard definition information, and therefore a user cannot create, change, or delete the file.

JP1/IM provides the `jcomonitorfcheck` command for checking the contents of the definition file for opening monitor windows.For details about this command, see *jcomonitorfcheck* in *Chapter 1. Commands*.

When the definitions are applied

The definition takes effect after JP1/IM - Manager is restarted or when the `jco_spmd_reload` command is executed. Note that the changes made to the definition while the user is logged in to JP1/IM - View or the Intelligent Integrated Management Base, are not applied. You need to restart JP1/IM - View or the Intelligent Integrated Management Base to apply the change.

Information that is specified

`@encode`

Specifies the character encoding that is to be used in the definition file for opening monitor windows. This item is optional.

To create an additional file for definition file for opening monitor windows, use an @encode statement to specify the character set for the definition file.

Item names will be expressed in characters that can be represented in the character encoding specified in the `@encode` statement. In addition, the definition file for opening monitor windows will be saved in the character encoding specified in the `@encode` statement.

In the following circumstances, item names displayed in JP1/IM - View or the Integrated Operation Viewer window, might be garbled:

- If the item name uses characters that cannot be represented in the character encoding specified in the `@encode` statement
- If the character encoding specified in the `@encode` statement does not match the character encoding in which the file was saved

If no @encode statement exists or if there is an error in the specified character set name that follows the @encode statement, the character set is determined automatically. However, depending on the contents of the definition file, the character encoding might not be determined correctly.

The specifiable character encodings are as follows:

- C
- EUCJIS
- SJIS
- UTF-8
- GB18030

Note

If you use UTF-8 as the encoding to save a definition file, save the file without attaching a BOM (byte order mark).

An error is output in the following cases:

- A character encoding other than C, EUCJIS, SJIS UTF-8 or GB18030 is specified
- The definition file does not begin with `@encode`.
- `@encode` is not followed by a character encoding specification.

Note

If you use a definition file for extended event attributes provided by another product, make sure the character encoding specified in the `@encode` statement matches the character encoding used in the definition file. In addition, if you will be transferring definition files, do not convert the character encoding of the definition files.

`DESC_VERSION=0300`

This is the table version record.

key-definition

Defines a fixed key in the event attributes that is to be used when a monitor window is opened. The key consists of three items:

- Event ID
- Product name
- Version

The combination of these attributes defines a link to operations and subkeys.

Format

`DEF_KEY PRODUCT_NAME="`*product-name*`"`

`EVENT_ID=`*event-ID*

`[VERSION=`*version*`|ALL]`

`{SUBKEY=`*subkey*

`|INTERFACE=`*interface-name*`}`

Arguments

• `PRODUCT_NAME="`*product-name*`"`

Specifies a product name as a character string, such as `/HITACHI/JP1/AJS`. This value must be the same as a value that is set in a `PRODUCT_NAME` extended attribute.

• `EVENT_ID=`*event-ID*

Specifies only the base part of an event identifier, expressed as eight hexadecimal characters. The extended part is ignored. If you need to include the extended part set for a JP1/SES event, use a subkey.

• `VERSION=`*version*

Specifies a version. The version specified in this argument is compared with the `ACTION_VERSION` JP1 event extended attribute. The version can be expressed in numeric characters (from `0` to `9`), alphabetic characters (`A` to `Z`), the forward slash (`/`), and the hyphen (`-`). The alphabetic characters are not case sensitive.

Specify a single version as a string of no more than 8 bytes. To specify a range of versions, separate the start version from the end version with a hyphen (`-`). In this case, there must be at least one space preceding and following the hyphen.

The version specified here cannot duplicate any version specified in any other key definition.

• `SUBKEY=`*subkey*

Specifies the name of a subkey. This parameter and the `INTERFACE` parameter are mutually exclusive.

If you specify the `SUBKEY` parameter, you need the subkey definition corresponding to the subkey name specified for `SUBKEY`, and the association definition.

• `INTERFACE=`*interface-name*

Specifies an interface name. For the key to define, specify only one interface that is to be used when the monitor window opens. This parameter and the `SUBKEY` parameter are mutually exclusive.

If you specify the `INTERFACE` parameter, you cannot use the subkey definition and association definition.

Notes:

The versions are compared in ascending order. If the start version is greater than the end version, that key definition is ignored even though no error is issued.

The value specified in `PRODUCT_NAME` must be the same as the value specified in a `PRODUCT_NAME` JP1 event extended attribute.

subkey-definition

When the monitor window is opened, the subkey definition is linked from the fixed key and registers the event attributes as the key.

Format

`DEF_SUBKEY`

`NAME=`*subkey-name*

`KEYS=`*attribute-name-1* `[,` *attribute-name-2*`[,`*attribute-name-3*`[,`*attribute-name-4*`]]]`

Arguments

- `NAME=`*subkey-name*

Specifies a name for the subkey, expressed using from 1 to 16 alphanumeric characters; no spaces or control characters can be used. This name is not case sensitive.

- `KEYS=`*attribute-name-1* `[,`*attribute-name-2* `[,`*attribute-name-3* `[,`*attribute-name-4*`]]]`

Specifies attribute names. The following table shows the specification formats of the attribute names.

Table 2–67: Specification formats of the attribute names

Specification format	Value format	Description
`B.ARRIVEDTIME`	13-digit decimal character string	Arrived time (time in milliseconds since UTC 1970-01-01 at 00:00:00)
`B.DESTSERVER`	Character string	Target event server name
`B.GROUPNAME`	Character string	Source group name
`B.IDBASE`	8 hexadecimal characters	Base part of the event ID
`B.IDEXT`	8 hexadecimal characters	Extended part of the event ID
`B.PROCESSID`	Decimal character string	Source process ID
`B.SEQNO`	Decimal character string	Sequence number in the database
`B.SOURCESEQNO`	Decimal character string	Sequence number by source
`B.SOURCESERVER`	Character string	Event-issuing server name
`B.TIME`	13-digit decimal character string	Registered time (time in milliseconds since UTC 1970-01-01 at 00:00:00)
`B.USERNAME`	Character string	Source user name
`B.MESSAGE`	Character string	Message
`E.JP1_SOURCEHOST`#	Character string	Event source host name
`E.`*xxxxxxx*	Character string	Extended attribute

#

A business group name cannot be used for the event-issuing server name (`B.SOURCESERVER`) and the event source host name (`E.JP1_SOURCEHOST`). If a business group name is specified, it is treated as a host name.

association-definition

Defines the association between subkey values and the interface.

Format

```
DEF_IF_RELATION
SUBKEY_NAME=subkey-name
{ VALUE1="attribute-value-1"[[ VALUE2="attribute-value-2"]...]
|KEY_DEFAULT }
IF_NAME=interface-name
```

Arguments

- SUBKEY_NAME=*subkey-name*

Specifies the name of the subkey. Express the name using from 1 to 16 alphanumeric characters; no spaces or control characters can be used. This name is not case sensitive.

- VALUE*n*="*attribute-value*"

Specifies an attribute value and its sort order. Specify for *n* an integer in the range from 1 to 4 representing the sort order among the attributes specified in the KEYS parameter in the subkey definition. The key values must match exactly. A regular expression cannot be used for the value. For a list of the specifiable attributes and their specification formats, see the explanation of *subkey-definition*.

If any of the attributes, such as VALUE1, VALUE2, ..., does not match, the interface specified in KEY_DEFAULT is used for the corresponding JP1 event.

- KEY_DEFAULT

Specify this argument instead of VALUE1, VALUE2, ..., in order to create an association with the interface when there is not an exact match with the values specified in VALUE1, VALUE2, ...

- IF_NAME=*interface-name*

Specifies the name of the interface that is to be called when the subkey values match. Express the interface name using from 1 to 16 alphanumeric characters; no spaces or control characters can be used. This name is not case sensitive.

call-interface-definition

Defines the interface to be used when a monitor window is opened.

Format

```
DEF_MTR_CALL
NAME=interface-name
EXEC_ID=application-execution-definition-identifier
PATH="command-arguments"
[PARAM=attribute-name-1[,attribute-name-2...]]
```

Arguments

- NAME=*interface-name*

Specifies a name for the interface. Express the name using from 1 to 16 alphanumeric characters; no spaces or control characters can be used. This name is not case sensitive.

- EXEC_ID=*application-execution-definition-identifier*

Specifies the identifier for an application execution definition. You must specify an identifier defined in the definition file for executing applications on the viewer.

You can launch the default browser by specifying "default_browser" for the EXEC_ID parameter. If you specify "default_browser" for the EXEC_ID parameter, specify a URL for the PATH parameter.

Note that a character string beginning with jco_ cannot be used because it is reserved as the application execution definition identifier.

- PATH="*command-arguments*"

Specifies command arguments that are to be passed to the executable file specified in `EXEC_ID`. The command line is formed by the name of the executable file specified in `EXEC_ID` and the arguments specified here. For example, you would specify `arg1` and `arg2` in the `PATH` parameter to form the following command line:

```
"app.exe arg1 arg2"
```

You can also specify in the `PATH` parameter reserved keywords that will be replaced with values from the viewer's operating environment attributes and event attributes. The following lists and describes the specifiable substitute keywords.

Table 2–68: Specifiable substitute keywords

Keyword	Substituted value
`%JCO_JP1USER%`	Central Console or the Intelligent Integrated Management Base are login user name
`%JCO_INSTALL_PATH%`#	Name of the viewer installation folder
`%IM_EVC_PARAMETER_`*n*`%`	Event attribute value specified in `PARAM` (*n*: integer of 1 or greater)
`%IM_EVC_LANGUAGE%`	Depending on the language environment, the language switches between `Japanese` and `English`.

#: In the Intelligent Integrated Management Base, the string is not substituted.

- `PARAM=`*attribute-name-1* `[,`*attribute-name-2*`...]`

Specifies the names of event attributes whose values are to be set. Sequential numbers that begin with 1 are assigned to the attribute names. This sequence corresponds to *n* in the substitute keywords.

Separate multiple event attributes with the comma, as shown in the example below:

```
B.EXTID,E.A0
```

You can specify some of the basic attributes and extended attributes. For details about the specifiable attributes and their specification formats, see the explanation of *subkey-definition*.

Example definition

This example opens a monitor window from the JP1 event that traps the Windows event log:

Note:

In this example, a line number is assigned at the beginning of each line for explanatory purposes.

```
1  DESC_VERSION=0300
2  #/HITACHI/JP1/NTEVENT_LOGTRAP 0600 TO
3  # Operating version
4  # 0600 FROM NT VERSION JP1/NTEVENT_LOGTRAP 0600 TO
5  DEF_KEY PRODUCT_NAME="/HITACHI/JP1/NTEVENT_LOGTRAP/NETMDM" EVENT_ID=00003A71 SUBKEY=SAMPLE
6  DEF_SUBKEY NAME=SAMPLE KEYS=E.A5
7  DEF_IF_RELATION SUBKEY_NAME=SAMPLE VALUE1="8010" IF_NAME=NETM_DM
8  DEF_MTR_CALL NAME=NETM_DM EXEC_ID=HITACHI_NETM_DM PATH="netmdm_argument"
```

Line 1

Indicates the character encoding used for the definition file. In this example, the character encoding is UTF-8.

Line 2

`DESC_VERSION=0300` means that the description format version of this file is `0300`.

Lines 3 to 5

These are comment lines. We recommend that you include the scope of the operating version.

Line 6

This is a key definition record. It means that if the product name is `/HITACHI/JP1/NTEVENT_LOGTRAP` and the event ID is `00003A71`, then the subkey `SAMPLE` is used to determine which monitor window is opened.

Line 7

This is a subkey definition record. It declares that the extended attributes PRODUCT_NAME and A5 (Windows event log ID) are used with the subkey name SAMPLE.

Line 8

This is an association definition record. It means that if the value of subkey E.A5 matches 8010, the interface NETM_DM is used to display the monitor window.

Line 9

This is a call interface definition record. It means that the interface name is NETM_DM and the argument netmdm_argument is passed to the command whose application execution definition identifier is HITACHI_NETM_DM, which is then executed.

Email environment definition file (jimmail.conf)

Format

```
Charset=email-character-encoding
From=sender-email-address
DefaultTo=default-destination-email-address[,default-destination-email-addre
ss...]
SmtpServer=SMTP-server-name
SmtpPort=SMTP-port-number
AuthMethod=authentication-method-when-sending-email
SmtpAuthPort=SMTP-AUTH-authentication-submission-port-number
Pop3Server=POP3-server-name
Pop3Port=POP3-port-number
AuthUser=authentication-account-name
AuthPassword=authentication-password
ConnectTimeout=network-connection-timeout-period
SoTimeout=communication-timeout-period
MailSubjectCutting=email-subject-drop-setting
MailNewLine=email-linefeed-code
```

File

`jimmail.conf` (email environment definition file)

`jimmail.conf.model` (model file of the email environment definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\mail`

For a logical host:

shared-folder`\JP1Cons\conf\mail`

Description

The email environment definition file is a definition file that sets information required to send an email, including email server host names, authentication methods, authentication account names, and passwords.

When the definitions are applied

The definition takes effect when the `jimmail` command is executed.

Information that is specified

The following rules are applied to the email environment definition file:

- Each entry must be specified on a line in *parameter-name=setting-value* format. On each line, *parameter-name* and *setting-value* are separated by the first equal sign (`0x3d`).
- Only `CR` (`0x0d`) + `LF` (`0x0a`) is treated as a line break. If line break codes other than `CRLF` are contained, the line break codes are converted to `CRLF` before output when a password is set by using the `jimmailpasswd` command.

- The parameter name is case sensitive.
- A line beginning with `#` (`0x23`) or Δ`#` is a comment statement. However, if there is a character other than a single-byte space (`0x20`) or a tab (`0x09`) before `#`, the line is not treated as a comment statement (Δ indicates a single-byte space or a tab).
- Single-byte spaces or tabs are treated as follows (Δ indicates a single-byte space or a tab):
  - Single-byte spaces or tabs immediately before or after a parameter name are ignored.

    Example: Δ*parameter-name*Δ=*setting-value*
  - Single-byte spaces or tabs immediately before or after the setting value are ignored. However, they are treated as characters and not ignored for the `AuthPassword` parameter.

    Example: *parameter-name*=Δ*setting-value*Δ
- If an invalid parameter is written, an error occurs. Also, if there is no equal sign (=) after a parameter name, an error occurs.

`Charset=`*email-character-encoding*

Defines the character encoding for the subject and text of an email to send.

The character encoding is not case sensitive.

The following table lists the initial values for the `Charset` parameter, and a value to be set if the value for the `Charset` parameter is not obtained.

Table 2–69: Initial values for the Charset parameter and setting values when the value could not be obtained

Environment	Initial value	Setting value when the value could not be obtained
Japanese environment	`iso-2022-jp`	`iso-8859-1`
Non-Japanese environment	`iso-8859-1`	`iso-8859-1`

The following table lists the character encoding that can be specified for `Charset`.

If you specify character encoding that cannot be specified, the setting value in the above table is assumed.

Table 2–70: Character encoding that can be specified for Charset

Character encoding	Description
`iso-2022-jp`	JIS encoding
`shift_jis`	Shift-JIS encoding
`euc-jp`	EUC encoding
`utf-8`	UTF-8 encoding
`iso-8859-1`	Latin1 encoding
`us-ascii`	ANSI encoding
`GB18030`	GB18030 encoding (GBK range only)
Others	Cannot be specified

If there is no parameter, the parameter does not have a value, or character encoding that cannot be specified for the parameter is defined, the `KAVB8715-W` message is output, and the initial value is set.

`From=`*source-email-address*

Defines the source email address of an email notification.

The initial value is the null character ("").

Only one source email address can be defined.

This item cannot be omitted.

Specify the source email address from 1 to 256 bytes.

The following table lists the permitted characters.

Table 2–71: Character encoding that can be used for From

Characters that can be used	Description
One-byte alphanumeric characters	`0` to `9`, and `a` to `z`
`@`	At mark (`0x40`)
`.`	Period (`0x2e`)
`-`	Hyphen (`0x2d`)
`_`	Underscore (`0x5f`)

If there is no essential parameter, the parameter does not have a value, a character that cannot be specified for a parameter is defined, a parameter is not in the RFC822 format, or a parameter is exceeding the maximum length, the `KAVB8714-E` message is output and the operation terminates abnormally.

`DefaultTo=`*default-destination-email-address*`[,`*default-destination-email-address*`...]`

Defines the default destination email address.

The initial value is the null character ("").

You can define 20 destination email addresses. To specify multiple email addresses, separate them by a comma (`,`).

A single-byte space or tab between an email address and a comma (`,`) is ignored.

Consecutive commas (`,`) are treated as a comma, and commas at the beginning and at the end are ignored. If the same email address is specified more than once, the email message is sent to the specified address only once.

This parameter can be omitted. If omitted, the `-to` option of the *jimmail* command must be specified.

If both the `DefaultTo` parameter and the `-to` option of the `jimmail` command are specified, the `-to` option is prioritized.

Specify the destination email address from 1 to 256 bytes.

The characters that can be used for the source email address can be used.

If unusable characters are specified, the parameter is not in the RFC822 format, or the parameter exceeds the maximum length, the `KAVB8714-E` message is output, and the operation terminates abnormally.

Also, if neither the `DefaultTo` parameter nor the `-to` option of the `jimmail` command is specified, the `KAVB8712-E` message is output, and the operation terminates abnormally.

`SmtpServer=`*SMTP-server-name*

Defines the host name or the IP address of the SMTP server to connect when sending an email. Configure one of the following files to enable successful host name resolution of *SMTP-server-name*:

- The `jp1hosts` file in JP1/Base on the manager host
- The `jp1hosts2` file in JP1/Base on the manager host
- The `hosts` file or DNS

For the IP address, only IPv4 addresses can be specified. IPv6 addresses cannot be specified.

The initial value of the `SmtpServer` parameter is the null character ("").

Specify only one SMTP server name across the system.

This parameter cannot be omitted.

Specify 1 to 255 of one-byte characters for the host name.

If there is no essential parameter, the parameter does not have a value, a character that cannot be used for a parameter is defined, or the parameter exceeds the maximum length, the KAVB8714-E message is output, and the operation terminates abnormally.

SmtpPort=*SMTP-port-number*

Defines the port number of the communication port for the SMTP server.

The initial value for the SmtpPort parameter is 25. If you could not obtain the value, 25 is assumed. Specify the port number from 1 to 65535.

If you define NONE or POP for AuthMethod, this item takes effect.

If there is no parameter, the parameter does not have a value, a character other than a numeric value is specified for the parameter, or a value outside the range is specified for the parameter, the KAVB8715-W message is output. The command continues processing, assuming the initial value.

AuthMethod=*authentication-method-for-sending-email*

Defines the authentication method for sending an email.

This parameter cannot be omitted.

Use the value listed in the table below for the authentication method. The initial value is NONE.

Table 2–72: Authentication method for AuthMethod

Value of AuthMethod	Authentication method
NONE	No authentication
POP	POP before SMTP authentication
SMTP	SMTP-AUTH authentication

Depending on the authentication method for sending an email, the items that must be set for the email environment definition file vary.

If there is no essential parameter, the parameter does not have a value, or a value outside the range is specified for the parameter, the KAVB8714-E message is output, and the operation terminates abnormally.

The following table lists the setting items for each AuthMethod value.

Table 2–73: Setting items when AuthMethod is NONE

Parameter name	Setting	Omission	Value assumed when omitted
Charset	Y	Possible	iso-8859-1
From	Y	Impossible	--
DefaultTo	Y	Possible	""
AuthMethod	Y	Impossible	--
SmtpServer	Y	Impossible	--
SmtpPort	Y	Possible	25
SmtpAuthPort	N	--	--
Pop3Server	N	--	--
Pop3Port	N	--	--
AuthUser	N	--	--
AuthPassword	N	--	--
ConnectTimeout	Y	Possible	10,000

Parameter name	Setting	Omission	Value assumed when omitted
SoTimeout	Y	Possible	10,000
MailSubjectCutting	Y	Possible	OFF
MailNewLine	Y	Possible	CRLF

Legend:

Y: Must be set.

N: Not necessary to be set.

Table 2–74: Setting items when AuthMethod is POP

Parameter name	Setting	Omission	Value assumed when omitted
Charset	Y	Possible	iso-8859-1
From	Y	Impossible	--
DefaultTo	Y	Possible	""
AuthMethod	Y	Impossible	--
SmtpServer	Y	Impossible	--
SmtpPort	Y	Possible	25
SmtpAuthPort	N	--	--
Pop3Server	Y	Impossible	--
Pop3Port	Y	Possible	110
AuthUser	Y	Impossible	--
AuthPassword	Y	Impossible	--
ConnectTimeout	Y	Possible	10,000
SoTimeout	Y	Possible	10,000
MailSubjectCutting	Y	Possible	OFF
MailNewLine	Y	Possible	CRLF

Legend:

Y: Must be set.

N: Not necessary to be set.

Table 2–75: Setting items when AuthMethod is SMTP

Parameter name	Setting	Omission	Value assumed when omitted
Charset	Y	Possible	iso-8859-1
From	Y	Impossible	--
DefaultTo	Y	Possible	""
AuthMethod	Y	Impossible	--
SmtpServer	Y	Impossible	--
SmtpPort	N	--	--
SmtpAuthPort	Y	Impossible	587
Pop3Server	N	--	--

Parameter name	Setting	Omission	Value assumed when omitted
`Pop3Port`	N	--	--
`AuthUser`	Y	Impossible	--
`AuthPassword`	Y	Impossible	--
`ConnectTimeout`	Y	Possible	`10,000`
`SoTimeout`	Y	Possible	`10,000`
`MailSubjectCutting`	Y	Possible	`OFF`
`MailNewLine`	Y	Possible	`CRLF`

Legend:

Y: Must be set.

N: Not necessary to be set.

`SmtpAuthPort=`*SMTP-AUTH-authentication-submission-port-number*

Defines the submission port number of the communication port for the SMTP-AUTH authentication. The initial value is `587`. If you cannot obtain the value, `587` is assumed. Specify a value from 1 to 65535.

When using the SMTP-AUTH authentication, specify the number of the destination port used by the SMTP server to connect for the `SmtpAuthPort` parameter if the connection email server does not use the submission port.

When you define `SMTP` for `AuthMethod`, this item takes effect.

If this parameter does not exist, the parameter does not have a value, characters other than numeric values are specified for the parameter, or a value outside the range is specified for the parameter, the `KAVB8715-W` message is output. The command continues processing, assuming the initial value.

`Pop3Server=`*POP3-server-name*

Defines the host name or the IP address of the POP3 server to be used for POP before SMTP authentication. Configure one of the following files to enable successful host name resolution of *POP3-server-name*:

- The `jp1hosts` file in JP1/Base on the manager host
- The `jp1hosts2` file in JP1/Base on the manager host
- The `hosts` file or DNS

For the IP address, IPv4 addresses can be specified. IPv6 addresses cannot be specified.

If the email server serves as both the SMTP server and the POP3 server, specify the SMTP server name specified for `SmtpServer`.

Specify only one POP3 server name across the system.

Specify 1 to 255 one-byte characters as the host name of the POP3 server. The initial value is the null character (`""`). Characters you can use as the host name of the POP3 server are the characters that can be used for the host name of the SMTP server.

If you define `POP` for `AuthMethod`, this item takes effect. When it takes effect, you must specify this parameter.

If there is no essential parameter, the parameter does not have a value, characters that cannot be specified for the parameter are specified, or the parameter exceeds the maximum length, the `KAVB8714-E` message is output, and the operation terminates abnormally.

`Pop3Port=`*POP3-port-number*

Defines the port number of the communication port for the POP3 server to use for the POP before SMTP authentication.

The initial value for the parameter is `110`. If you cannot obtain the value, `110` is assumed. Specify a value from 1 to 65535 for the port number.

If you define `POP` for `AuthMethod`, this item takes effect.

If there is no parameter, the parameter does not have a value, characters other than numeric values are specified for the parameter, or a value outside the range is specified for the parameter, the `KAVB8715-W` is output, and the initial value is assumed.

`AuthUser=`*authentication-account-name*

The `AuthUser` parameter defines the authentication account name to use for the POP before SMTP or SMTP-AUTH authentication.

Specify 1 to 255 one-byte characters for the authentication account name.

The initial value is the null character (`""`).

If you specify `POP` or `SMTP` for the `AuthMethod` parameter, this item takes effect.

If there is no essential parameter, the parameter does not have a value, characters (multi-byte) that cannot be used for the parameter are defined, or the parameter exceeds the maximum length, the `KAVB8714-E` message is output, and the operation terminates abnormally.

`AuthPassword=`*authentication-password*

For the `AuthPassword` parameter, the authentication password for the POP before SMTP or SMTP-AUTH authentication is set.

The authentication password for the `AuthPassword` parameter is set by using the `jimmailpasswd` command.

If you edit the email environment definition file, and set a password in plain text for the `AuthPassword` parameter, you cannot log in to the email server because the authentication password does not match when connecting to the email server.

If you specify `POP` or `SMTP` for the `AuthMethod` parameter, this item takes effect.

If there is no essential parameter, the parameter does not have a value, characters (multi-byte) that cannot be used for the parameter are specified, or the parameter exceeds the maximum length, the `KAVB8714-E` message is output, and the operation terminates abnormally.

`ConnectTimeout=`*network-connection-timeout-period*

For the `ConnectTimeout` parameter, define the timeout period in milliseconds for waiting until connection between the SMTP and POP3 servers is established. The initial value is 10,000 milliseconds (10 seconds).

Specify 1,000 to 3,600,000 (1 to 3,600 seconds) for the timeout period.

Change this value only when a timeout occurs with the initial value according to the operating environment.

If there is no parameter, the parameter does not have a value, a character string other than numeric characters is specified for the parameter, or a value outside the range is specified for the parameter, the `KAVB8715-W` message is output, and the initial value is assumed.

`SoTimeout=`*communication-timeout-period*

Define the timeout period in milliseconds until a response is received from the SMTP and POP3 servers for the `SoTimeout` parameter. The initial value is 10,000 milliseconds (10 seconds).

Specify a value from 1,000 to 3,600,000 (1 to 3,600 seconds) as the timeout period.

Only when a communication timeout error occurs with the initial value, change the value according to the operating environment.

If there is no parameter, the parameter does not have a value, a character string other than numeric characters is specified for the parameter, or a value outside the range is specified for the parameter, the `KAVB8715-W` message is output, and the initial value is assumed.

`MailSubjectCutting=`*email-subject-drop-setting*

For the `MailSubjectCutting` parameter, define whether to drop the email subject, and forcibly send the email if the email subject exceeds the maximum length when sending the email.

- When `OFF` is set, the email subject is not dropped, and the `jimmail` command terminates abnormally.

- When ON is set, drops the email subject according to the character encoding specified for the Charset parameter within 512 bytes, and continues sending the email.

The initial value is OFF. The setting value is not case sensitive.

If there is no parameter, the parameter does not have a value, or a value other than ON and OFF is specified, the KAVB8715-W message is output, and the initial value is assumed.

MailNewLine=*email-linefeed-code*

For the MailNewLine parameter, define the linefeed code to be used in the text of an email. The jimmail command replaces the linefeed code (\n) specified for the optional argument of the command with the linefeed code specified for this parameter before sending the email. The initial value is CRLF.

The setting value is not case sensitive.

The linefeed code is regulated as CRLF in RFC. Do not change the initial value if you do not have specific reasons. On some email servers, if linefeed codes other than CRLF are used, email messages might not be sent, or a line in email contents might not be broken.

The linefeed codes are defined by using the values listed in the following table.

Table 2–76: Setting value for MailNewLine

Setting value	Description
CRLF	CR (0x0d) + LF (0x0a)
LF	LF (0x0a)
CR	CR (0x0d)

If there is no parameter, the parameter does not have a value, or a value outside the range is defined for the parameter, the KAVB8715-W message is output, and the initial value is assumed.

Example

The following is the email environment definition file for a Japanese environment immediately after installation:

```
Charset=iso-2022-jp
From=
DefaultTo=
SmtpServer=
SmtpPort=25
AuthMethod=NONE
SmtpAuthPort=587
Pop3Server=
Pop3Port=110
AuthUser=
AuthPassword=
ConnectTimeout=10000
SoTimeout=10000
MailSubjectCutting=OFF
MailNewLine=CRLF
```

The following is the email environment definition file for a non-Japanese environment immediately after installation:

```
Charset=iso-8859-1
From=
DefaultTo=
SmtpServer=
SmtpPort=25
AuthMethod=NONE
SmtpAuthPort=587
Pop3Server=
Pop3Port=110
AuthUser=
AuthPassword=
ConnectTimeout=10000
SoTimeout=10000
MailSubjectCutting=OFF
MailNewLine=CRLF
```

Display message change definition file (jcochmsg.conf)

Format

```
DESC_VERSION=1
# Display-message-change-definition-comment
def definition-name-1
    [cmt comment]
    [define {enable | disable}]
    [addflag {true | false}]
    cnd
        event-condition
    end-cnd
    msg message
end-def

def definition-name-2
    [cmt comment]
    [define {enable | disable}]
    [addflag {true | false}]
    cnd
        event-condition
    end-cnd
    msg message
end-def
```

File

`jcochmsg.conf` (display message change definition file)

`jcochmsg.conf.model` (model file for the display message change definition file)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chattr\jcochmsg.conf`

For a logical host:

shared-folder`\jp1cons\conf\chattr\jcochmsg.conf`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chattr/jcochmsg.conf`

For a logical host:

shared-directory`/jp1cons/conf/chattr/jcochmsg.conf`

Description

This file defines the JP1 event conditions that change the display of a message using the display message change function and defines the message after the change. JP1 event attributes that match event conditions are changed in accordance with the definitions in this file. Specify this file using the language encoding that is used by JP1/IM - Manager.

The maximum size of this file is 22 megabytes (23,068,672 bytes).

There are two types of parameters in the display message change definition file:

- Display message change definition file version
  Defines the format version of the display message change definition file.
- Display message change definition parameter
  Defines a condition for the JP1 events whose display message is to be changed and the display message after the change. The higher a display message change definition appears in the display message change definition file, the higher its priority.

When the definitions are applied

The definition takes effect when the event display message change function is enabled, and one of the following operations is performed:

- JP1/IM - Manager is restarted
- The `jco_spmd_reload` command is executed
- The **OK** button is clicked in the Add Display Message Change Definition Settings window opened from the **Display Message Change Definition Settings** menu
- The **Apply** button is clicked in the View Display Message Change Definition window

Information that is specified (display message change definition file version)

`DESC_VERSION`

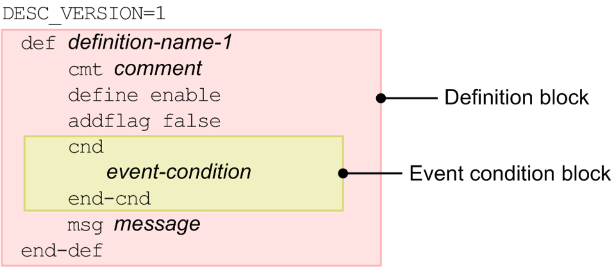
Specifies the file version that determines the format of this display message change definition file. Specify a value of 1. If `DESC_VERSION` is omitted, 1 is assumed as the file version.

Specify `DESC_VERSION` on the first line of the definition file (the first line in the file excluding any null lines and comment lines). If there is no file version in the first line, 1 is assumed.

Information that is specified (display message change definition parameter)

As shown in the following figure, the definition parameter for changing the display message consists of a definition block and an event condition block.

Figure 2–10: Definition parameter for changing the display message



```
DESC_VERSION=1
 def definition-name-1
     cmt comment
     define enable
     addflag false
     cnd
         event-condition
     end-cnd
     msg message
 end-def
```

Multiple definition blocks can be specified. The number of definition blocks that can be specified is from 0 to 3,000. If the number of definition blocks exceeds the maximum, message KAVB4640-W is output, and processing continues, ignoring the definition blocks after number 3,000.

`def` to `end-def` (definition block)

These are the start and end parameters for a display message change definition. The block from `def` to `end-def` can be omitted, in which case the system assumes that messages are not to be changed for any JP1 events.

After `def`, specify the names of display message change definitions. If you specify `def`△△△*definition-1*△△△*definition-2*△△△, then △△*definition-1*△△△*definition-2*△△△ are treated as the definition names (Δ indicates a single-byte space).

For a definition name, specify a character string of from 1 to 50 bytes. Each definition name must be unique within the display message change definition file. The permitted characters are all characters other than the control characters (from `0x00` to `0x1F` and `0x7F` to `0x9F`).

`cmt` *comment*

Describes the comment for the display message change definition. The comment specified for `cmt` is displayed in the comment section of the Display Message Change Definition Settings window. Only one `cmt` parameter can be specified in the definition block. This parameter can be omitted. Specify the comment using up to 1,024 bytes. The permitted characters are all characters other than the control characters (from `0x00` to `0x1F` and `0x7F` to `0x9F`).

`define {`<u>`enable`</u>` | disable}`

Specifies whether to enable the display message change definition. Only one `define` parameter can be specified in the definition block. To enable the display message change definition, specify `enable`, to disable it, specify `disable`. The `define` parameter can be omitted. By default, `enable` is set. The values are not case sensitive.

`addflag {true | `<u>`false`</u>`}`

Indicates an additional display message change definition has been added from a window, and specifies whether the display message change definition is an additional display message change definition. Therefore, to edit the additional display message change definition file, you do not need to specify the `addflag` parameter. Only one `addflag` parameter can be specified in the definition block. Specify `true` for the additional display message change definition, and `false` for the display message change definition. When `true` is specified, the icon (📎) is displayed in **Type** of the View Display Message Change Definition window. The `addflag` parameter can be omitted. By default, `false` is set. The values are not case sensitive.

`cnd` to `end-cnd` (event condition block)

These are the start and end parameters for the block that specifies a condition for the JP1 events whose display message is to be changed. You must specify at least one event condition block in a definition block. The event condition block cannot be omitted. If a received JP1 event satisfies multiple event conditions, the definition block closest to the beginning of the display message change definition file is used. Tabs and spaces before and after the `cnd` and `end-cnd` parameters are ignored.

event-condition

Specifies a condition for the JP1 events whose display message is to be changed. You can specify from 1 to 256 event conditions per event condition block. When multiple event conditions are specified, it is assumed that they are connected with the AND condition. Specify an event condition in the following format (Δ indicates a single-byte space):

*attribute-name*Δ*comparison-keyword*Δ*operand* `[`Δ*operand*`] ...`

Note that a line consisting of only spaces or tabs is ignored during processing.

attribute-name

Specifies the name of the attribute that you want to compare. To specify a basic attribute, place `B.` immediately before the name. To specify an extended attribute (common information or user-specific information), place `E.` immediately before the name. Uppercase and lowercase are distinguished.

The following table lists and describes the combinations of attribute names and comparison keywords and the operands that can be specified.

Table 2–77: Combinations of attribute names and comparison keywords and the operands that can be specified

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	`B.ID`	• `Match` • `Does not match`	A maximum of 100 of these items can be specified. Specify the event ID in hexadecimal notation. Letter case is ignored. The permitted range is from `0` to `7FFFFFFF`.
2	Reason for registration	`B.REASON`	• `Match` • `Does not match`	A maximum of 100 of these items can be specified.
3	Source process ID	`B.PROCESSID`	• `Match` • `Does not match`	A maximum of 100 of these items can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
4	Source user ID	`B.USERID`	• `Match` • `Does not match`	A maximum of 100 of these items can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
5	Source group ID	`B.GROUPID`	• `Match` • `Does not match`	A maximum of 100 of these items can be specified. The permitted range is from -2,147,483,648 to 2,147,483,647.
6	Source user name	`B.USERNAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
7	Source group name	`B.GROUPNAME`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
8	Event-issuing server name (source host)#1	`B.SOURCESERVER`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
9	Destination event server name#1	`B.DESTSERVER`	• `First characters` • `Match`	A maximum of 100 of these items can be specified, unless a regular expression

No.	Item	Attribute name	Comparison keyword	Operand
			• Does not match • Is contained • Is not contained • Regular expression	is used, in which case only one item is allowed.
10	Message	B.MESSAGE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
11	Severity	E.SEVERITY	Match	Multiple items can be specified, unless a regular expression is used, in which case only one item is allowed. Only the following values can be specified: Emergency, Alert, Critical, Error, Warning, Notice, Information, or Debug.
12	User name	E.USER_NAME	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
13	Product name	E.PRODUCT_NAME	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
14	Object type	E.OBJECT_TYPE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
15	Object name	E.OBJECT_NAME	• First characters • Match • Does not match • Is contained • Is not contained	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• Regular expression	
16	Root object type	E.ROOT_OBJECT_TYPE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
17	Root object name	E.ROOT_OBJECT_NAME	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
18	Object ID	E.OBJECT_ID	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
19	Occurrence	E.OCCURRENCE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
20	Result code	E.RESULT_CODE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.
21	Event source host name#1	E.JP1_SOURCEHOST	• First characters • Match • Does not match • Is contained • Is not contained	A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• Regular expression	
22	Program-specific extended attribute#2	E.*xxxxxxx*	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	For the attribute name, you can specify a name with a maximum length of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_). A maximum of 100 of these items can be specified, unless a regular expression is used, in which case only one item is allowed.

#1

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is Match or Do not match, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than Match and Do not match is selected, a business group name specified in a path format is treated as a host name.

If the -ignorecasehost option of the jcoimdef command is set to ON, and a comparison keyword other than Regular expression is selected, the character string is no longer case sensitive.

#2

You can also specify a JP1 product-specific extended attribute. For example, the program-specific extended attribute for the JP1/AJS job execution host is E.C0. For details about the product-specific extended attributes, consult the documentation for the products that issue JP1 events.

comparison-keyword

Specifies one of BEGIN (begins with), IN (matches), NOTIN (does not match), SUBSTR (includes), NOTSUBSTR (does not include), or REGEX (regular expression) as the comparison keyword. The comparison keyword is case sensitive.

operand

Specifies a character string as the value that is to be compared with the attribute value as specified by the comparison keyword. Operands are case sensitive.

Separate multiple operands with one or more consecutive spaces or a tab. The OR condition is applied to the specified operands. Note that if a regular expression is specified, only one operand can be specified.

To specify a single-byte space, a tab, end-of-line code (CR or LF), or % as part of an operand, specify as follows:

No.	Value to be set	How to specify
1	Tab (0x09)	%09
2	Space (0x20)	%20
3	% (0x25)	%25
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.IDΔINΔ100Δ200
```

Legend: Δ indicates a single-byte space (0x20)

You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length of operands in bytes that are specified in the event condition block).

msg

This parameter describes the message to be displayed.

You must specify one msg parameter in a definition block. The parameter cannot be omitted.

The msg parameter cannot exceed 1,023 bytes. The permitted characters are all characters other than the control characters (from 0x00 to 0x1F and 0x7F to 0x9F).

If a msg parameter is specified outside of the definition block, message KAVB4629-W is output, the msg parameter specification is ignored, and processing continues.

In the circumstances listed below, message KAVB4631-W is output, and processing continues, ignoring the definition block that produced the error.

- The msg parameter is omitted
- The msg parameter is specified more than once
- The message specified in the msg parameter exceeds 1,023 bytes
- The message specified in the msg parameter includes control characters

To specify a variable in the message after the change, use a format such as $EVSEV. The variable will be replaced with the actual value of the attribute value in the event.

The following table describes the available variables.

Type of information	Variable name	Description
Information contained in the basic attributes of JP1 events	EVBASE	Entire basic event information#1
	EVID	Event ID (*basic-code*:*extended-code*)
	EVIDBASE	Event ID (basic code)
	EVDATE	Event registration date (*YYYY*/*MM*/*DD*)#2
	EVTIME	Event registration time (*hh*:*mm*:*ss*)#2
	EVPID	Event source process ID
	EVUSRID	User ID of the event source process
	EVGRPID	Group ID of the event source process
	EVUSR	Event source user name
	EVGRP	Event source group name
	EVHOST	Event source host name
	EVIPADDR	Event source IP address
	EVSEQNO	Serial number
	EVARVDATE	Event arrival date (*YYYY*/*MM*/*DD*)#2
	EVARVTIME	Event arrival time (*hh*:*mm*:*ss*)#2
	EVSRCNO	Serial number at the event source
	EVMSG	Entire message text#3
	EVDETAIL	Entire detailed event information#3, #4
Information contained in the extended attributes of JP1 events	EVSEV	Severity levels in extended event information (Emergency, Alert, Critical, Error, Warning, Notice, Information, Debug)#3
	EVUSNAM	User name#3

Type of information	Variable name	Description
	`EVOBTYP`	Object type[#3]
	`EVOBNAM`	Object name[#3]
	`EVROBTYP`	Registration type[#3]
	`EVROBNAM`	Root object name[#3]
	`EV"PRODUCT_NAME"`	Product name[#5]
	`EV"OBJECT_ID"`	Object ID[#5]
	`EV"OCCURRENCE"`	Occurrence[#5]
	`EV"START_TIME"`	Start time[#5]
	`EV"END_TIME"`	End time[#5]
	`EV"RESULT_CODE"`	Return code[#5]
	`EV"JP1_SOURCEHOST"`	Issuing host name[#5]
	`EV"`*extended-attribute-name*`"`	Any extended attribute[#5]
Other	`EV"@JP1IM_CORRELATE"`	Correlation event flag • Not a correlation event: `0` • Correlation approval event: `1` • Correlation failure event: `2`
	`EV"@JP1IM_ORIGINAL_SEVERITY"`	Severity levels in extended event information (before change) (`Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, `Debug`)[#3]
	`EV"@JP1IM_CHANGE_SEVERITY"`	New severity level flag • Severity is not changed: `0` • Severity is changed: `1`
	`ACTHOST`	Value of the manager host name[#3]
	`EVENV1` to `EVENV20`	Data obtained by specifying parantheses (`()`) in a regular expression in the specification of an event condition[#5] (applicable only when an extended regular expression is used at the manager host)

#1

The basic information of a JP1 event is converted to the following format and passed to the message after the change (Δ indicates a single-byte space):

event-ID Δ *event-source-user-name* Δ *event-source-user-ID* Δ *event-source-group-name* Δ *event-source-group-ID* Δ *event-source-event-server-name* Δ *event-source-process-ID* Δ *event-registration-date* Δ *event-registration-time* Δ *event-source-host-IP-address*

An item that is not set is replaced with the null character.

#2

This attribute value is converted using the time zone set for JP1/IM - Manager and is passed to the message after the change.

#3

When the message is changed, if the applicable attribute does not exist, the variable is converted to a null character and passed to the message after the change.

#4

When detailed attribute information for a JP1 event is in binary format, the variable is converted to a null character and passed to the message after the change.

#5

If the applicable attribute does not exist, the character string of the variable is passed as-is to the message after the change.

Notes about specifying variables

- If you want to specify `$` as a character, specify the escape character `\` before the `$`.
- If you specify a character, such as an alphanumeric character or an underscore (_), immediately after the variable name, the variable will not be converted correctly. In such a case, enclose the variable name in curly brackets (`{ }`), as shown in the examples below. These examples assume that `100:0` is specified as the event ID (`$EVID`) and `ABC` is specified as the extended attribute `EX` (`$EV"EX"`).

  Examples:

  display-message-change-definition -> *information-after-conversion*

  `$EVID abc` -> `100:0 abc`

  `$EVIDabc` -> `$EVIDabc`

  `${EVID}abc` -> `100:0abc`

  `$EVID_abc` -> `$EVID_abc`

  `${EVID}_abc` -> `100:0_abc`

  `$EV"EX" abc` -> `ABC abc`

  `$EV"EX"abc` -> `ABCabc`
- If a non-variable name is specified, no information will be converted at that location. For example, if you specify `$AAA` but there is no variable `AAA`, `$AAA` will be set in the message after the change.
- If the value of the attribute specified in `EV"`*extended-attribute-name*`"` or `EVENV1` to `EVENV20` cannot be acquired, no information will be converted at that location. For example, if `$EV"BBB"` is specified but the JP1 event has no extended attribute `BBB`, `$EV"BBB"` will be set in the message after the change.
- If the value of the attribute specified in a variable other than `EV"`*extended-attribute-name*`"` or `EVENV1` to `EVENV20` cannot be acquired, the variable will be converted to the null character at that location. For example, if `$EVSEV` is specified but the JP1 event has no extended attribute `SEVERITY`, the null character will be set in the message after the change.
- When there is more than one event condition that uses a regular expression, and when there is more than one set of parentheses (`()`) in a regular expression, the data captured in parentheses is associated with variables `EVENV1` to `EVENV20` in a nested sequential manner, proceeding from left to right within each regular expression, and then through each event condition in series.

Conversion functions for inherited event information

- Inherited event information can be converted into character strings of a user-specified length. This makes it possible to display lists of message IDs, dates, and so on in an easy-to-read format where the data is aligned in a fixed-length field.

  If the length of the inherited event information is less than the length specified by the user, single-byte spaces are added to make it the specified length.

  If the length of the inherited event information is greater than the length specified by the user, the information is truncated to make it fit the length specified by the user.

  When multi-byte characters are truncated, the truncation is performed in such a way that characters are not broken. If the length after truncation is less than the length specified by the user, a single-byte space is added.

  Specification format:

  ```
  $variable-name$FIXLEN=number-of-bytes
  ```

Specify a numeric value from 1 to 1,023 for *number-of-bytes*. If the specification format is incorrect, `$FIXLEN=`*number-of-bytes* will be treated as a character string.

By enclosing *variable-name* in curly brackets (`{}`), you can explicitly specify the material to be treated as part of the parameter.

No.	Specification format	Character string in $variable-name	Character string set in message	Remarks
1	`$`*variable-name*`$FIXLEN=6`	`ABC`	`ABC△△△`	Because the character string is shorter than the specified length, single-byte spaces are added to compensate.
2		`ABCDEFG`	`ABCDEF`	Because the character string exceeds the specified length, it is truncated.
3	`$`*variable-name*`$FIXLEN=1024`	`ABC`	`ABC$FIXLEN=1024`	Because the specified value exceeds the maximum value of `1023`, it is treated as a character string.
4	`$`*variable-name*`$FIXLEN=10225`	`ABC`	`ABC`Δ ... Δ 5, where Δ ... Δ represents 1,019 Δ characters	Only the first four characters in the character string after `$FIXLEN=` are considered part of the parameter, so the fifth and subsequent characters are treated as a character string.
5	`${`*variable-name*`$FIXLEN=10}235`	`ABC`	`ABC△△△△△△△235`	The material in the curly brackets (`{}`) through `10` is treated as the parameter, and `235` is treated as a character string.

Legend: Δ indicates a single-byte space

- It is possible to align the number of digits of numerical values to be displayed in the message by padding the value with zeros. This can be used when you want to convert the numeric value representing seconds to a format such as *ss*, *ss*`.`*sss*, or *ss*`.`*ssssss*.

  Specification format:

  ```
  $variable-name$FIXNUM=00.000000
  ```

  You can specify 0 to 2 digits for the integer portion and 0 to 6 digits for the decimal portion.

  This conversion is also possible when the value stored in the variable is a character string representation of a numeric value.

  When a character string representing a non-numeric value is set, no conversion is performed if the integer portion exceeds the specified number of digits, or the value stored in the variable is greater than or equal to 100.

  When the decimal portion exceeds the specified number of digits, the excess decimal places are truncated. Truncation is also performed whenever 7 or more decimal places are set in the value stored in the variable.

No.	Specification format	Character string in $variable-name	Character string set in message	Remarks
1	`$`*variable-name*`$FIXNUM=00.000`	`1`	`01.000`	The integer and decimal portions are padded with zeros.
2		`123.123456`	`123.123456`	No conversion is performed because the value is greater than or equal to 100.
3	`$`*variable-name*`$FIXNUM=0.00`	`15`	`15.00`	The integer portion is not converted because it exceeds the specified number of digits (1).
4	`$`*variable-name*`$FIXNUM=00`	`1`	`01`	The integer portion is padded with zeros.
5		`1.5`	`01`	The decimal portion exceeds the specified number of digits, so the excess decimal places are truncated.

No.	Specification format	Character string in $variable-name	Character string set in message	Remarks
6	$*variable-name*$FIXNUM=00.000000	0.1234567	00.123456	The 7th and subsequent decimal places are truncated.
7	$*variable-name*$FIXNUM=.00	1	1.00	The decimal portion is padded with zeros.
8	$*variable-name*$FIXNUM=00.	1	01	The integer portion is padded with zeros.
9	$*variable-name*$FIXNUM=ABC	1	1$FIXNUM=ABC	The invalid $FIXNUM specification is treated as a character string.
10	$*variable-name*$FIXNUM=0.00	ABC	ABC	No conversion is performed because the value in $*variable-name* is non-numeric.
11		0.0000000A	0.0000000A	

- The number of seconds elapsed since 1970/01/01 is converted to character strings representing the year, month, day, hour, minute, and seconds.

  The conversion uses the time zone of the manager host.

  No conversion is performed unless the value stored in the variable is a character string representing a numeric value from 0 to 4,102,444,799.

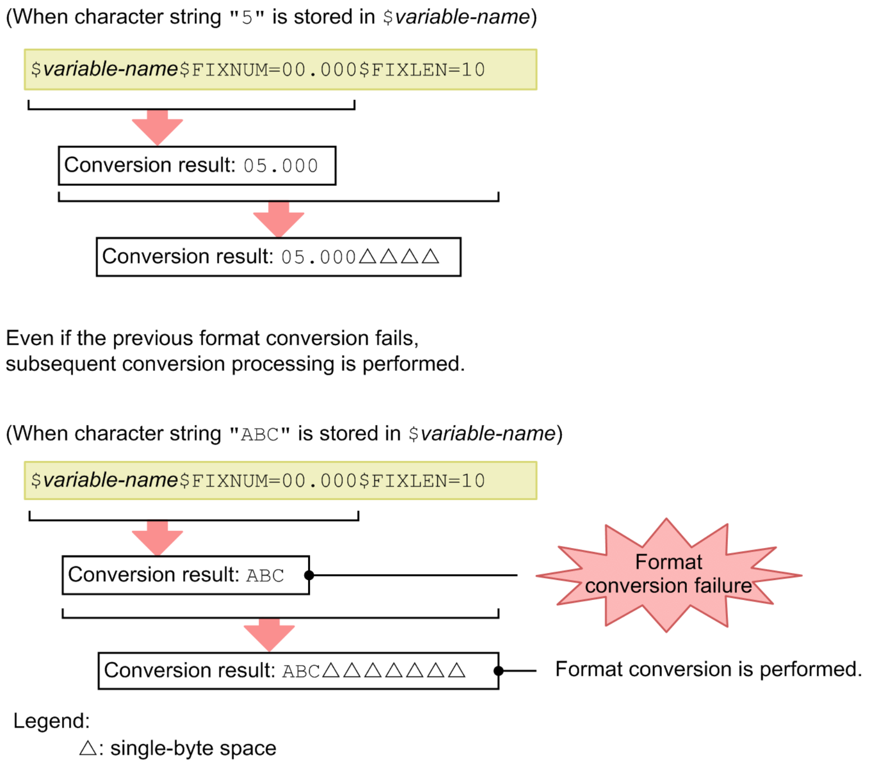
No.	Specification format	Conversion
1	$*variable-name*$YEAR	Converts the number of seconds elapsed since 1970/01/01 to a year. After conversion, the value is output in the format *YYYY*. The year to be output is padded with zeros as necessary to make it 4 digits.
2	$*variable-name*$MONTH	Converts the number of seconds elapsed since 1970/01/01 to a month After conversion, the value is output in the format *MM*. The month to be output is padded with zeros as necessary to make it 2 digits.
3	$*variable-name*$DAY	Converts the number of seconds elapsed since 1970/01/01 to a day. After conversion, the value is output in the format *DD*. The day to be output is padded with zeros as necessary to make it 2 digits.
4	$*variable-name*$HOUR	Converts the number of seconds elapsed since 1970/01/01 to an hour. After conversion, the value is output in the format *hh*. The hour to be output is padded with zeros as necessary to make it 2 digits. The hour value is output in 24-hour format.
5	$*variable-name*$MIN	Converts the number of seconds elapsed since 1970/01/01 to a minute. After conversion, the value is output in the format *mm*. The minutes value to be output is padded with zeros as necessary to make it 2 digits.
6	$*variable-name*$SEC	Converts the number of seconds elapsed since 1970/01/01 to seconds. After conversion, the value is output in the format *ss*. The seconds value to be output is padded with zeros as necessary to make it 2 digits.

- Successive format conversion functions can be specified.

  If you specify a succession of format conversion functions, the format conversions will be performed from left to right in the order specified.

  Even if the previous format conversion fails, subsequent conversion processing is performed.

Figure 2–11: Successive format conversions


(When character string "5" is stored in $variable-name)
$variable-name$FIXNUM=00.000$FIXLEN=10
Conversion result: 05.000
Conversion result: 05.000△△△△
Even if the previous format conversion fails, subsequent conversion processing is performed.
(When character string "ABC" is stored in $variable-name)
$variable-name$FIXNUM=00.000$FIXLEN=10
Conversion result: ABC
Format conversion failure
Conversion result: ABC△△△△△△△
Format conversion is performed.
Legend:
△: single-byte space

# *comment-line*

A line beginning with a hash mark (#) is treated as a comment. Note that the comment will be deleted if the display message change definition is set from JP1/IM - View.

Example definition

If the event ID matches `100` or `200`, the severity is `Warning`, and the source host matches `hostA`, `hostB`, or `hostC`, change the message to `A failure occurred in the database server`, with the date and time prepended to the beginning of the message.

```
DESC_VERSION=1
def display-message-change-1
    cmt comment1
    define enable
    addflag false
    cnd
        B.ID IN 100 200
        E.SEVERITY IN Warning
        B.SOURCESERVER IN hostA hostB hostC
    end-cnd
    msg $EVDATE $EVTIME A failure occurred in the database server
end-def
```

The following example extracts the message ID and message text portions from the Hntr log.

```
DESC_VERSION=1
def display-message-change-1
    cmt comment1
    define enable
    addflag false
    cnd
        E.OBJECT_TYPE IN LOGFILE
        E.OBJECT_NAME SUBSTR HNTRLib2
        E.ROOT_OBJECT_TYPE IN LOGFILE
        E.PRODUCT_NAME IN /HITACHI/JP1/NT_LOGTRAP
        B.MESSAGE REGEX [0-9]{4}%20[0-9]{4}/[0-9]{2}/[0-9]{2}%20[0-9]{2}:[0-
9]{2}:[0-9]{2}\.[0-9]{3}[%20]+.*[%20]+[0-9A-Z]+%20[0-9A-Z]+[%20]+([^%20]+)[%
20]+(.*)
    end-cnd
    msg $EVENV1 $EVENV2
end-def
```

The following example prepends a character string to the beginning of all messages for a particular product.

```
DESC_VERSION=1
    def display-message-change-1
    cmt comment1
    define enable
    addflag false
    cnd
        E.PRODUCT_NAME IN PRODUCT_A
    end-cnd
    msg [Product A]$EVMSG
end-def
```

Display item definition file for a display message change definition (chmsg_attr_list.conf)

Format

```
# comment-line
attribute-name
attribute-name
   :
   :
attribute-name
```

File

`chmsg_attr_list.conf` (display item definition file for a display message change definition)

`chmsg_attr_list.conf.model` (model file for the display item definition file for a display message change definition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chattr\attr_list`

For a logical host:

shared-folder`\jp1cons\conf\chattr\attr_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chattr/attr_list`

For a logical host:

shared-directory`/jp1cons/conf/chattr/attr_list`

Description

This definition file specifies the items to be displayed in the **Attribute name** display area of the Display Message Change Definition Settings window. The display items specified in the display item definition file for a display message change definition are displayed in the **Attribute name** display area of the Display Message Change Definition Settings window in the order they are specified.

When the definitions are applied

The definitions take effect when Central Console is started and when the definitions are re-read by executing the `jco_spmd_reload` command.

Information that is specified

# *comment-line*

A line beginning with a hash mark (#) is treated as a comment.

attribute-name

The items to be displayed in the **Attribute name** display area of the Display Message Change Definition Settings window are specified in the display item definition file for a display message change definition.Write one attribute name corresponding to a display item on each line. You can specify from 0 to 256 display items.

Uppercase and lowercase are distinguished. Space and tab characters specified at the beginning or the end of the attribute name are ignored.

When `SEPARATOR` is specified, a horizontal line such as `--------------------` is displayed in the **Attribute name** display area of the Display Message Change Definition Settings window. `SEPARATOR` can be used to separate frequently used items from those used less frequently.

However, if only `SEPARATOR` is specified, only `--------------------` will appear in the **Attribute name** display area. If you then select `--------------------`, you will be unable to set the attribute name.

The following table lists the attribute names that can be specified.

Table 2–78: List of display items

No.	Display item	Attribute name
1	Event source host name#	`E.JP1_SOURCEHOST`
2	Registered host name	`B.SOURCESERVER`
3	Event level	`E.SEVERITY`
4	Object type	`E.OBJECT_TYPE`
5	Object name	`E.OBJECT_NAME`
6	Root object type	`E.ROOT_OBJECT_TYPE`
7	Root object name	`E.ROOT_OBJECT_NAME`
8	Occurrence	`E.OCCURRENCE`
9	User name	`E.USER_NAME`
10	message	`B.MESSAGE`
11	Product name	`E.PRODUCT_NAME`
12	Event ID	`B.ID`
13	Destination event server name	`B.DESTSERVER`
14	Program-specific extended attribute	`OTHER_EXTENDED_ATTRIBUTE`
15	Reason for registration	`B.REASON`
16	Source process ID	`B.PROCESSID`
17	Source user name	`B.USERNAME`
18	Source user ID	`B.USERID`
19	Source group name	`B.GROUPNAME`
20	Source group ID	`B.GROUPID`
21	Object ID	`E.OBJECT_ID`
22	Return code	`E.RESULT_CODE`
23	`--------------------`	`SEPARATOR`

Note:

If an attribute name is specified twice, both specifications are ignored.

If the display item definition file for a display message change definition cannot be read, or the number of valid display items is 0, items 1 to 22 are displayed.

#

If the user mapping function of the event source host is not enabled, this item is cannot be displayed in the Display Message Change Definition Settings window.

Example definition

```
E.JP1_SOURCEHOST
B.SOURCESERVER
E.SEVERITY
E.OBJECT_TYPE
E.OBJECT_NAME
E.ROOT_OBJECT_TYPE
E.ROOT_OBJECT_NAME
E.OCCURRENCE
E.USER_NAME
B.MESSAGE
E.PRODUCT_NAME
B.ID
B.DESTSERVER
OTHER_EXTENDED_ATTRIBUTE
B.REASON
B.PROCESSID
B.USERNAME
B.USERID
B.GROUPNAME
B.GROUPID
E.OBJECT_ID
E.RESULT_CODE
```

Automatic input definition file for a display message change definition (chmsg_auto_list.conf)

Format

```
# comment-line
[DEFAULT_NAME display-message-change-definition]
attribute-name
attribute-name
   :
   :
attribute-name
attribute-name
```

File

`chmsg_auto_list.conf` (automatic input definition file for a display message change definition)

`chmsg_auto_list.conf.model` (model file for the automatic input definition file for a display message change definition)

Storage directory

In Windows

For a physical host:

Console-path`\conf\chattr\auto_list`

For a logical host:

shared-folder`\jp1cons\conf\chattr\auto_list`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/chattr/auto_list`

For a logical host:

shared-directory`/jp1cons/conf/chattr/auto_list`

Description

This file defines the JP1 event attributes that are set automatically when the Add Display Message Change Definition Settings window opens. The window opens when the user selects it from the **Display Message Change Definition Settings** menu after selecting a JP1 event from the list of events in the Event Console window and selecting **View**. You can also define a default name for the display message change definition.

When the definitions are applied

The contents of the definition file take effect when Central Console is started and when the definitions are re-read by executing the `jco_spmd_reload` command.

Information that is specified

# *comment-line*

A line beginning with a hash mark (#) is treated as a comment.

DEFAULT_NAME *display-message-change-definition*

Specifies the identifier that defines the display message change definition. The identifier must be on the first line in the file (the first line in the file that is not a null line or a comment line).

The display message change definition specified for this parameter is displayed as the initial value when the Add Display Message Change Definition Settings window opens. The window opens when the user selects it from the **Display Message Change Definition Settings** menu after selecting a JP1 event from the list of events in the Event Console window and selecting **View**.

For the name, specify a character string of up to 40 bytes. The permitted characters are all characters other than the control characters (from 0x00 to 0x1F and 0x7F to 0x9F). If a name with more than 40 bytes is specified, characters after the 40th are dropped, and the first 40 bytes of the character string are used as the display message change definition. If this parameter is omitted, Add display message change definition is assumed as the display message change definition.

attribute-name

For the automatic input definition file for a display message change definition,specify the attribute of a JP1 event that is to be set as an event condition when the Add Display Message Change Definition Settings window opens. The window opens when the user selects it from the **Display Message Change Definition Settings** menu after selecting a JP1 event from the list of events in the Event Console window and selecting **View**. At this time, the condition for the attribute name specified for this parameter will be displayed as the initial value.

For the definition items, write one attribute name of a JP1 event that will be set on each line.

Uppercase and lowercase are distinguished. Space and tab characters specified at the beginning or the end of the attribute name are ignored.

If there are no valid attribute names, the KAVB1952-W message is output to the integrated trace log file, and the default items are used.

If the same attribute name is specified twice, both are ignored, and the KAVB1954-W message is output to the integrated trace log file.

The order in which the attributes are written in this definition file determines the order in which JP1 event attributes are displayed automatically in the **Event conditions** section of the Display Message Change Definition Settings window.

If *attribute-name* is specified incorrectly, the KAVB1953-W message is output to the integrated trace log file, and the attribute name is ignored.

The following table lists the attribute names that can be specified.

Table 2–79: List of display items

No.	Display item	Attribute name
1	Event source host name#	E.JP1_SOURCEHOST
2	Registered host name	B.SOURCESERVER
3	Event level	E.SEVERITY
4	Object type	E.OBJECT_TYPE
5	Object name	E.OBJECT_NAME
6	Root object type	E.ROOT_OBJECT_TYPE
7	Root object name	E.ROOT_OBJECT_NAME
8	Occurrence	E.OCCURRENCE
9	User name	E.USER_NAME
10	Message	B.MESSAGE

No.	Display item	Attribute name
11	Product name	E.PRODUCT_NAME
12	Event ID	B.ID
13	Destination event server name	B.DESTSERVER
14	Reason for registration	B.REASON
15	Source process ID	B.PROCESSID
16	Source user name	B.USERNAME
17	Source user ID	B.USERID
18	Source group name	B.GROUPNAME
19	Source group ID	B.GROUPID
20	Object ID	E.OBJECT_ID
21	Return code	E.RESULT_CODE

Note:

If an attribute name is specified twice, both specifications are ignored.

If the definition file cannot be read, or the number of valid display items is 0, items 1 to 12 are displayed.

#

If the user mapping function of the event source host is not enabled, this item is cannot be displayed in the Add Display Message Change Definition Settings window.

Example definition

```
DEFAULT_NAME display-message-change-definition
E.JP1_SOURCEHOST
B.SOURCESERVER
E.SEVERITY
B.MESSAGE
E.PRODUCT_NAME
B.ID
```

Environment definition file for events after the display message is changed (chmsgevent.conf)

Format

```
[logical-host-name\JP1CONSOLEMANAGER]
"SEND_CHANGE_MESSAGE_EVENT"=dword:hexadecimal-value
```

File

`chmsgevent.conf.update` (model file for the environment definition file for events after the display message is changed)

Storage directory

In Windows

Console-path`\default\`

In UNIX

`/etc/opt/jp1cons/default/`

Description

This file defines the execution environment of the function for issuing an event after a display message has been changed. It specifies whether to enable the function.

The required definitions are provided as a model file. To change the settings, copy the model file and edit the copy after renaming the copy to definition file (for Windows: *console-path*`\conf\chmsgevent.conf`, for UNIX: `/etc/opt/jp1cons/conf/chmsgevent.conf`).

When the definitions are applied

The definitions take effect when JP1/IM - Manager is restarted after the `jbssetcnf` command has been executed in JP1/Base to apply the definitions to the JP1 common definition information.

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER]`

Indicates the key name of the JP1/IM - Manager environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for a physical host and *logical-host-name* for a logical host.

`"SEND_CHANGE_MESSAGE_EVENT"=dword:`*hexadecimal-value*

Specifies whether to enable the function to issue an event after a display message is changed.

- `00000001`: Enabled (issue an event after a display message is changed)
- `00000000`: Disabled (do not issue an event after a display message is changed)

The default value is `00000000` (disabled).

Example definition

```
[JP1_DEFAULT\JP1CONSOLEMANAGER]
"SEND_CHANGE_MESSAGE_EVENT"=dword:00000000
```

Web page call definition file (hitachi_jp1_product-name.html)

Format

```
<HTML>
<HEAD>
<META HTTP-EQUIV="refresh" CONTENT="0;URL=URL-of-other-product's-web-page">
</HEAD>
</HTML>
```

File

`hitachi_jp1_`*product-name*`.html` (Web page call definition file)

`hitachi_jp1_`*product-name*`.html.model` (model file for the Web page call definition file)

Storage directory

View-path`\conf\webdata\en\`

Description

This file is used for calling another product's Web page from the Tool Launcher.

When another product's Web page is to be called from the Tool Launcher, the Web page call definition file is referenced first and then its URL defined in this file is accessed. If you plan to call some other product's web page from the Tool Launcher, you must set its URL by editing this file as appropriate to your environment.

If you attempt to display a Web page from the Tool Launcher without having set its URL, a page describing the setting method is displayed.

List of Web page call definition files

JP1/IM provides the definition files listed in the table below. See the individual linked product documentation for details about the versions and operating systems that support the linked product.

Table 2–80: List of Web page call definition files that correspond to item names in the Tool Launcher window

Item in the Tool Launcher window			Web page call definition file name	Product name
Folder name	Subfolder name	Function name		
`Network Management`	--	`Network Node Manager`	`hitachi_jp1_cm2.html`	HP NNM Version 7.5 or earlier
				HP NNM
`Inventory/ Software Distribution`	--	`Integrated Asset Management`	`hitachi_jp1_assetinfomationmanager.html`	JP1/Asset Information Manager
	--	`Inventory/ Software Distribution`#	`hitachi_jp1_netmdm.html`	JP1/Software Distribution Manager
`Storage Management`	`Storage Area`	`Storage System Usage Management`	`hitachi_jp1_hicommand_tuning_manager.html`	JP1/HiCommand Tuning Manager

Item in the Tool Launcher window			Web page call definition file name	Product name
Folder name	Subfolder name	Function name		
	Management	Storage Hardware Management	hitachi_jp1_hicommand_device_manager.html	JP1/HiCommand Device Manager
		Storage Resource Allocation Management	hitachi_jp1_hicommand_provisioning_manager.html	JP1/HiCommand Provisioning Manager
		Storage Replication Management	hitachi_jp1_hicommand_replication_manager.html	Hitachi Replication Manager
		Tiered Storage Resource Management	hitachi_jp1_hicommand_tiered_storage_manager.html	JP1/HiCommand Tiered Storage Manager
		Global Input/output Path Availability Management	hitachi_jp1_hicommandGLAM.html	JP1/HiCommand Global Link Availability Manager
Server Management	--	Web Console	hitachi_jp1_systemmanager.html	JP1/ Server Conductor

Legend:

--: None

#

JP1/IM - View for Windows cannot link with the Web page versions of JP1/Software Distribution Manager.

By changing the URLs specified in these HTML files to the URLs of individual product Web pages, you can access those products' Web pages from the Tool Launcher window.

When the definitions are applied

The definition takes effect when JP1/IM - View is restarted.

Information that is specified

`<META HTTP-EQUIV="refresh" CONTENT="0;URL=`*URL-of-other-product's-web-page*`">`

Specifies the URL of another product's Web page.

If you attempt to display another product's Web page from the Tool Launcher without setting its URL, a page describing the setting method is displayed (*View-path*`\conf\webdata\en\webconfig_hitachi_jp1_`*product-name*`.html`). You can specify the URL by following the instructions provided on the displayed page.#

#

- The URL set on this page is the default value. With some products, the user can customize the URL. Check the URLs used by other products beforehand.

  Sometimes, the URL of a product will have changed, for a reason such as upgrading. If no window opens at the specified URL, check the applicable product's documentation.

- In *host name*, specify the host name or IP address of the machine where the product corresponding to the Web page is installed.

Example definition

```
<HTML>
<HEAD>
<META HTTP-EQUIV="refresh" CONTENT="0;URL=http://hostA/OvCgi/ovlaunch.exe">
</HEAD>
</HTML>
```

Definition file for the Tool Launcher window

Format

```
@file type="definition-file-type", version="definition-format-version";
# comment-line
@define-block type="function-tree-def";
folder-definition
function-definition
@define-block-end;
```

File

`!JP1_CC_FTREE0.conf` (definition file for the Tool Launcher window)

`!JP1_CC_FTREE0.conf.model` (model file for the definition file for the Tool Launcher window)

Storage directory

View-path`\conf\function\en\`

Description

This file defines tree and item information to be displayed in the Tool Launcher window of JP1/IM - View.

JP1/IM provides the `jcofuncfcheck` command for checking the contents of the definition file for the Tool Launcher window. For details about this command, see *jcofuncfcheck (Windows only)* in *Chapter 1. Commands*.

When the definitions are applied

The definition takes effect after JP1/IM - View is restarted.

Information that is specified

`@file type="function-definition"`

Declares that this is a definition file for the Tool Launcher window. This statement is mandatory.

You must always specify `function-definition`.

This statement must be on the first line of the file.

`version="0300";`

Specify `0300` for the version.

`#` *comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

`@define-block type="function-tree-def"; to @define-block-end;`(Tool Launcher definition block)

Tool Launcher definition block

Creates folders or functions that are to be displayed in the Tool Launcher window and specifies application execution definition identifiers to associate the application that is to be executed when a function is chosen.

The functions are displayed in the Tool Launcher window in the order of their file names. Within the same file, the functions are displayed in the order of their definition blocks. You can change the display order of menu items by changing the order of the file names or definition blocks.

The statements that can be specified in this block depend on whether folders or functions are being defined:

Table 2–81: Statements

When folders are defined	When functions are defined
`id` statement `parent_id` statement `name` statement	`id` statement `parent_id` statement `name` statement `execute_id` statement `icon` statement `arguments` statement

If any other statement is specified, an error is output but only the extraneous statement is ignored.

The following describes these statements.

`id="`*menu-identifier*`";`

Defines a menu identifier for the menu tree definition block. This statement is mandatory. This statement can be specified only once in a block.

If the file to be analyzed contains multiple blocks with the same `id`, their priority is determined as follows and only the block that has the highest priority is effective:

1. Last block when the file names are sorted in ascending order

2. Last block in the file

All other blocks are ignored.

Express a menu identifier using from 1 to 32 alphanumeric characters. This character string must be unique within the definition file for the Tool Launcher window. To achieve uniqueness, observe the following naming rules:

- When defining folders

company-name`[`*_product-name*`]`

- When defining functions

company-name_product-name`[`*_function-name-(or-window-name)*`]`

If an appropriately named folder name already exists, do not add a new folder; use the definition file storage location folder already specified in the other definition file.

`"root"` cannot be used because it is reserved for the highest menu identifier.

A character string beginning with `jco_` cannot be used because it is reserved as an application execution identifier.

`parent_id="`*parent-menu-identifier*`";`

Specifies `root` or the menu identifier that is located above the local menu identifier in the tree configuration. You can specify a maximum of 3 hierarchical levels, including `root`. This statement is mandatory. This statement can be specified only once in a block.

You cannot specify multiple parent menu identifiers to create multiple higher folders.

`name="`*display-name*`";`

Defines the name that is to be displayed in the Tool Launcher window. This statement is mandatory. This statement can be specified only once in a block.

Specify in *display-name* the character string that is to be displayed in the Tool Launcher window; we recommend that you use a simple but readily understood name. The character string can contain Japanese characters.

We recommend that you use a noun phrase, such as the character string `Command Execution Function`, because the specified value is displayed in the menu.

Although this value need not be unique in the definition, we recommend that you assign a unique name to eliminate possibilities for confusion.

`execute_id="`*application-execution-definition-identifier*`";`

Specifies the identifier for the application execution definition that is to be executed when the function displayed in the Tool Launcher window is double-clicked. If you specify a function, this statement is mandatory. You can specify this statement only once in a block.

You can launch the default browser by specifying `"default_browser"` for the `execute_id` parameter. If you specify `"default_browser"` for the `execute_id` parameter, specify a URL in the `arguments` parameter.

If you are creating a folder, this statement is ignored if specified.

If the specified application execution definition identifier does not exist, the menu is not displayed.

Note that a character string beginning with `jco_` cannot be used, because it is reserved as the application execution definition identifier.

`icon="`*display-icon-file-name*`";`

Specifies the file that contains the icon that is to be displayed in the Tool Launcher window. Specify the full path name of a GIF file. The recommended size for the GIF image is 16 × 16 pixels. If the specified icon image is not this size, it will be resized when the icon is displayed.

You can specify this statement only when you are specifying a function.

If you are creating a folder, this statement is ignored if specified.

If this statement is omitted, the common icon is used.

`arguments="`*command-arguments*`";`

Specifies arguments for the application specified in `execute_id`. You can use this statement only when you are specifying a function. You can specify this statement only once in a block.

You can also set in `arguments` reserved keywords that will be replaced with the viewer's operating environment attributes or alternate strings for substitution from registry values. For details about alternate strings, see *Alternate string* in *Definition file for executing applications* in *Chapter 2. Definition Files*.

If you are creating a folder, this statement is ignored if specified.

The full path of the executable file specified in `execute_id` is linked with the value of `arguments` obtained from the alternate string with a single-byte space added.

Arguments are linked to command line with ["] omitted from before and after

command-arguments. In this case, the command cannot be executed if its length exceeds 1,024 characters.

To set string that includes single-byte space as arguments to application,enclose command-arguments with ["]. For example [arguments=""string""].

["] before and after command-arguments are omitted when linked to command line. Therefore, when starting Microsoft Edge with the Tool Launcher window, if arguments in alternate string that has been replaced include single-byte space, Microsoft Edge may not operates as intended.

To set string that includes single-byte space as arguments, enclosethe string with ["]. For example [arguments=""string""].

The following shows an example definition of a menu tree definition block:

```
@define-block type="function-tree-def";
id="hitachi_jp1";
parent_id="root";
name="Sample management";
@define-block-end;
@define-block type="function-tree-def";
id="hitachi_jp1_seihin_sample";
parent_id="hitachi_jp1";
name="Sample window";
```

```
icon="sample.gif";
execute_id="hitachi_jp1_seihin_sample_execute";
arguments="node_map";
@define-block-end;
```

Example definition

The following shows an example of the definition file for the Tool Launcher window:

```
#
# All Rights Reserved, Copyright (C) 2000, Hitachi, Ltd.
#
@file type="function-definition", version="0300";
#-----------------------------------------------------------
@define-block type="function-tree-def";
id="jco_folder_Network";
parent_id="root";
name="Network Management";
@define-block-end;
#-----------------------------------------------------------
@define-block type="function-tree-def";
id="jco_JP1_Cm2";
parent_id="jco_folder_Network";
name="Network Management";
icon="%JCO_INSTALL_PATH%\image\menu\cm2_manager.gif";
execute_id="default_browser";
arguments="%JCO_INSTALL_PATH%\conf\webdata\en\hitachi_jp1_cm2.html";
@define-block-end;
#-----------------------------------------------------------
@define-block type="function-tree-def";
id="jco_folder_JobSystemOperation";
parent_id="root";
name="Job System Management";
@define-block-end;
#-----------------------------------------------------------
@define-block type="function-tree-def";
id="jco_JP1_AJS2";
parent_id="jco_folder_JobSystemOperation";
name="Job System Management";
icon="%JCO_INSTALL_PATH%\image\menu\ajs2_manager.gif";
execute_id="jco_JP1_AJS2";
arguments="-t "%JCO_JP1TOKEN%"";
@define-block-end;
#-----------------------------------------------------------
```

Command button definition file (cmdbtn.conf)

Format

```
DESC_VERSION=file-version

#comment-line
def
  [usr target-user-name target-user-name ...]

  btn command-button-name
    [cmt comment-about-command-button]
    [cmdtype {agent|client}]
    [inev {true|false}]
    [hst target-host]
    cmd command-line
    [var environment-variable-file-name]
    [qui {true|false}]
    [preview {true|false}]
  end-btn
  :
  :
end-def
:
:
```

File

`cmdbtn.conf`

Storage directory

In Windows

For a physical host:

Console-path`\conf\console\rmtcmd\`

For a logical host:

shared-folder`\jp1cons\conf\console\rmtcmd\`

In UNIX

For a physical host:

`/etc/opt/jp1cons/conf/console/rmtcmd/`

For a logical host:

shared-directory`/jp1cons/conf/console/rmtcmd/`

Execution permission

In Windows

Administrators group and SYSTEM users

In UNIX

Users with the `root` permissions

Description

This file defines the command buttons to be displayed in the Execute Command window. The maximum size of the command button definition file is 10 megabytes. If there are multiple command button definitions that can be used, the definition listed first in the command button definition file is displayed.

When the definitions are applied

If the `jcoimdef` command has been executed to enable the command button, the command button definitions are applied when the Execute Command window opens.

Note that if you change the definition of the command button while JP1/IM - View is running, you must restart JP1/IM - View.

Information that is specified

`DESC_VERSION=`*file-version*

Specifies the version of the format of the command button definition file. The specifiable values are `1` and `2`. To use the functionality that inherits the client application or event information, specify `2`. When `2` is specified, the following parameters can be specified:

- `cmdtype`
- `inev`
- `preview`

When the file version is omitted or a numeric value other than `1` or `2` is specified, `1` is assumed.

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

`def` to `end-def` (definition block)

These are the start and end parameters of the command button definition. You can specify a maximum of 64 parameters.

`[usr` *target-user-name* *target-user-name* `...]`

Specifies the names of JP1 users who use the command button. The number of characters you can specify for each target user name is from 1 to 31 bytes. Only one-byte alphanumeric characters can be used. Alphabets are not case sensitive. To specify multiple names, separate the names by one or more consecutive spaces or tabs. You can specify a maximum of 100 target user names. Target user names from the 101st are ignored. If this parameter is omitted, all JP1 users become target users. One target user name can be specified between `def` and `end-def`. No target user names can be specified between `btn` and `end-btn`.

`btn` *command-button-name* to `end-btn`

Specify the start and the end of a command button. *command-button-name* is displayed as the name of a command button in the Execute Command window. You can specify a maximum of eight characters for *command-button-name*. Specifiable characters are characters other than control characters (`0x00` to `0x1F`, `0x7F` to `0x9F`). The command button name is case sensitive. A maximum of 16 command buttons can be specified in a definition block. The same command button name cannot be specified twice. If *command-button-name* exceeds the limit for number of characters or the same command button name is specified twice, the command button name cannot be loaded.

`[cmt` *comment-about-command-button*`]`

Provides a description of the command button. The comment is displayed as a tool tip. This parameter can be omitted. You can specify a maximum of 40 characters for the comment. Characters from the 41st are ignored. You can specify any characters.

[cmdtype {agent|client}]

Specifies the type of command executed by a command button. Select whether the button will be used for managed-host commands or by client applications. Client applications are executed by the client application execution functionality. If you specify this parameter, specify 2 for DESC_VERSION.

For command execution on an agent or a manager host, specify the agent parameter. For command execution by a client application, specify the client parameter.

If you specify client for cmdtype, you cannot specify the hst and var parameters.

agent and client are not case sensitive.

[inev {true|false}]

Specifies whether to inherit event information by using the command button. If you specify this parameter, specify 2 for DESC_VERSION.

Specify true to execute the command by inheriting event information specified when you click the command button, or specify false not to execute the command. If this parameter is omitted, false is assumed.

true and false are not case sensitive.

[hst *target-host*]

Specifies the name of the host on which the command is executed. For *target-host*, you can specify a host name, host group name, business group name, or monitoring group name.

For a host name or a host group name, you can specify a character string with a maximum of 255 bytes. For a business group name or a monitoring group name, you can specify a character string with a maximum of 2,048 bytes. This parameter can be omitted.

If the integrated monitoring database and the IM Configuration Management database are enabled, the business group name can be specified in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and you specify the business group name in a path format, the name is treated as a host name or a host group name.

Specify a variable to hold the inherited event information. For details about the inherited event information that can be specified, see *4.19.5(1) Specifiable event inheritance information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. To specify inheritance of event information, specify true for the inev parameter. If you make this specification, make sure that the length of the character string following replacement of the variable with JP1 event information is equal to or less than the maximum number of bytes permitted for *target-host*. If the length of the character string exceeds the limit, a truncated character string is specified as the target host name in the environment variable file.

cmd *command-line*

Specifies the command to be executed. You can specify a maximum of 4,096 bytes for the command line. This parameter cannot be omitted.

Specify a variable to hold the inherited event information. To specify inheritance of event information, specify true for the inev parameter. If you make this specification, make sure that the length of the character string following replacement of the variable with JP1 event information is equal to or less than the maximum number of bytes permitted for *target-host*. If the length of the character string exceeds the limit, a truncated character string is specified as the target host name in the environment variable file.

[var *environment-variable-file-name*]

Specifies the name of the environment variable file in which the environment variable of the command to be executed is specified. This parameter can be omitted. For details about the environment variable file format, see the *JP1/Base User's Guide*. You can specify a character string with a maximum of 255 bytes for the environment variable file name. If the environment variable file name exceeds the limit, the command button is not loaded.

Specify a variable for the inherited event information. To specify inherited event information, specify true for the inev parameter. When you specify inherited event information, make sure that the length of a character string following replacement of the variable with JP1 event information is equal to or less than the maximum number of bytes permitted for the environment variable file. If the length of the character string exceeds the limit, a truncated character string is specified as the target host name in the environment variable file.

`[qui {true|false}]`

Specifies whether to display a message confirming that the command can be executed before executing a command with a command button. If the confirmation message is not displayed, the command is executed at the same time the command button is clicked.

Specify `true` if you want the confirmation message to be displayed. Specify `false` if you do want the message to be displayed. If this parameter is omitted, `false` is assumed. However, if `true` is specified for the `preview` parameter, the Preview Command Execution Content window opens.

`true` and `false` are not case sensitive.

`[preview {true|false}]`

If you inherit event information by using a command button, this parameter specifies whether to check the action definition of the command with the preview function after event information is inherited. To specify this parameter, specify 2 for `DESC_VERSION`.

Specify `true` to display the preview window. Specify `false` if you do not want to display the preview window. If this parameter is omitted, `true` is assumed.

`true` and `false` are not case sensitive.

This parameter is ignored if `false` is specified for the `inev` parameter.

If `false` is specified for the `preview` parameter and `true` is specified for the `qui` parameter, the command is executed at the same time the command button is clicked. The Preview Command Execution Content window and a message to confirm command execution are not displayed.

Example definition

```
DESC_VERSION=2

def
# Execute the command on the viewer host.
# Specify inherited event information for the command to be executed.
# Before executing the command, display the preview window.
  btn App1
    cmt Execute App1.
    cmdtype client
    inev true
    cmd C:\kansi\app1.exe $EVIDBASE $EVSEQNO "$EVMSG"
  end-btn

# Execute the command on the viewer host.
# Specify inherited event information for the command to be executed.
# Before executing the command, display the confirmation dialog box. The pre
view window is not displayed.
  btn App2
    cmt Execute App2.
    cmdtype client
    inev true
    cmd C:\kansi\app2.exe $EVIDBASE $EVSEQNO "$EVMSG"
    preview false
  end-btn

# Execute the command on the viewer host.
# Specify inherited event information for the command to be executed.
# Do not display the dialog box and the preview window before executing the
```

```
command.
  btn App3
    cmt Execute App3.
    cmdtype client
    inev true
    cmd C:\kansi\app3.exe $EVIDBASE $EVSEQNO "$EVMSG"
    qui true
    preview false
  end-btn

# Execute the command on the agent or the manager host.
# Specify inherited event information for the command to be executed.
# Display the preview window before executing the command.
  btn Cmd1
    cmt Execute cmd1.
    cmdtype agent
    inev true
    hst $EVHOST
    cmd /kansi/cmd1 $EVIDBASE $EVSEQNO '$EVMSG'
  end-btn

# Execute the command on the agent or the manager host.
# Do not specify inherited event information for the command to be executed.
# Display the confirmation dialog box before executing the command.
  btn Cmd2
    cmt Execute cmd2.
    hst agent2
    cmd /kansi/cmd2
  end-btn

end-def
```

Start program definition file (!JP1_CS_APP0.conf)

Format

```
@define-block type="application-execution-def";
id="program-identifier";
path="start-program-path";
@define-block-end;
```

File

`!JP1_CS_APP0.conf` (start program definition file)

`!JP1_CS_APP0.conf.model` (model file for the start program definition file)

Storage directory

View-path`\conf\sovtoolexec\en\`

Description

This file defines the start path for a program that is added to the toolbar in the Monitoring Tree window.

To add a program to the toolbar in the Monitoring Tree window, and then start the program from the toolbar, you must also edit the following definition files:

- Toolbar definition file
- Icon operation definition file

When the definitions are applied

The definition takes effect when the Monitoring Tree window is re-opened.

Information that is specified

From `@define-block type` to `@define-block-end;`

The information from `@define-block type` to `@define-block-end;` constitutes a single definition block. To add multiple programs to the toolbar in the Monitoring Tree window, specify this definition block as many times as there are programs to be added. You can specify the following parameters in this definition block:

`id="`*program-identifier*`"`

Specifies the identifier that indicates the program to be started. You can specify from 1 to 32 alphanumeric characters. This character string must be unique within the definition file. The program identifier specified in this parameter must be the same as a program identifier that is specified in the icon operation definition file (`!JP1_CS_FTREE0.conf`). For details about the icon operation definition file (`!JP1_CS_FTREE0.conf`), see *Icon operation definition file (!JP1_CS_FTREE0.conf)* in *Chapter 2. Definition Files*.

`path="`*start-program-path*`"`

Specifies the path of the program to be started. An executable file that can be specified must be an `.exe` or `.bat` file.

Example definition

```
#
# All Rights Reserved. Copyright (C) 2003, Hitachi, Ltd.
#
@file type="application-execution-definition", version="0300";
#----------------------------------------------------------
@define-block type="application-execution-def";
id="app_notepad";
path="C:\WINNT\NOTEPAD.EXE";
@define-block-end;
#----------------------------------------------------------
```

Toolbar definition file (!JP1_CS_FTOOL0.conf)

Format

```
@define-block type="function-toolbar-def";
toolbar="sov_JP1_IM_Central_Console|sov_JP1_IM_Function_Tree|sov_JP1_IM_Visu
al_View|sov_JP1_IM_Bmv_Help|icon-identifier...";
@define-block-end;
```

File

`!JP1_CS_FTOOL0.conf` (toolbar definition file)

`!JP1_CS_FTOOL0.conf.model` (model file for the toolbar definition file)

Storage directory

View-path`\conf\sovtoolitem\en\`

Description

This file defines the order of programs that are added to the toolbar in the Monitoring Tree window.

To add a program to the toolbar in the Monitoring Tree window, and then start the program from the toolbar, you must also edit the following definition files:

- Start program definition file
- Icon operation definition file

When the definitions are applied

The definition takes effect when the Monitoring Tree window is re-opened.

Information that is specified

From `@define-block type` to `@define-block-end;`

The information from `@define-block type` to `@define-block-end;` constitutes a single definition block. This block can be specified only once in the definition file.

`toolbar="sov_JP1_IM_Central_Console|sov_JP1_IM_Function_Tree|sov_JP1_IM_Visual_View|sov_JP1_IM_Bmv_Help|`*icon-identifier*`";`

Specifies the icon identifiers in the order they are to be displayed. The icon identifiers are separated by the vertical bar (`|`) and the icons are displayed from left to right in the Monitoring Tree window in the order they are specified here. An icon identifier is a character string consisting of no more than 32 alphanumeric characters. Each icon identifier character string must be unique within the definition file. The icon identifiers specified in this parameter must be the same as icon identifiers specified in the icon operation definition file (`!JP1_CS_FTREE0.conf`). For details about the icon operation definition file (`!JP1_CS_FTREE0.conf`), see *Icon operation definition file (!JP1_CS_FTREE0.conf)* in *Chapter 2. Definition Files*.

Example definition

```
#
# All Rights Reserved. Copyright (C) 2003, Hitachi, Ltd.
```

```
#
@file type="function-definition", version="0300";
#----------------------------------------------------------
@define-block type="function-toolbar-def";
toolbar="sov_JP1_IM_New_Info|sov_JP1_IM_Visual_View|sov_JP1_IM_Function_Tree
|sov_JP1_IM_Central_Console|sov_JP1_IM_Bmv_Help|tool_notepad";
@define-block-end;
#----------------------------------------------------------
```

Icon operation definition file (!JP1_CS_FTREE0.conf)

Format

```
@define-block type="function-tree-def";
id="icon-identifier";
name="tooltip";
iconstandard="icon-storage-path";
icondown="icon-storage-path";
iconrollover="icon-storage-path";
icondisable="icon-storage-path";
execute_id="program-identifier";
arguments="argument";
@define-block-end;
```

File

`!JP1_CS_FTREE0.conf` (icon operation definition file)

`!JP1_CS_FTREE0.conf.model` (model file for the icon operation definition file)

Storage directory

View-path`\conf\sovtoolitem\en\`

Description

This file defines the operation of icons that are displayed on the toolbar in the Monitoring Tree window.

To add a program to the toolbar in the Monitoring Tree window, and then start the program from the toolbar, you must also edit the following definition files:

- Start program definition file
- Toolbar definition file

When the definitions are applied

The definition takes effect when the Monitoring Tree window is re-opened.

Information that is specified

From `@define-block type` to `@define-block-end;`

Information from `@define-block type` to `@define-block-end;` constitutes a single definition block.

To add multiple programs to the toolbar in the Monitoring Tree window, specify this definition block as many times as there are programs to be added. In this definition block, you can specify the following parameters:

`id="`*icon-identifier*`";`

Specifies the identifier that indicates the appropriate icon. You can specify from 1 to 32 alphanumeric characters. This character string must be unique within the definition file. Also, the icon identifier specified for this parameter must be the same as the icon identifier specified for the toolbar definition file (`!JP1_CS_FTOOL0.conf`). For details about the toolbar definition file (`!JP1_CS_FTOOL0.conf`), see *Toolbar definition file (!JP1_CS_FTOOL0.conf)* in *Chapter 2. Definition Files*.

`name="`*tooltip*`";`

Specifies the tooltip that is to be displayed when the cursor is placed on the icon.

`iconstandard="`*icon-storage-path*`";`

Specifies the full path of the icon that is to be displayed during normal operation.

`icondown="`*icon-storage-path*`";`

Specifies the full path of the icon that is to be displayed when the icon is clicked.

`iconrollover="`*icon-storage-path*`";`

Specifies the full path of the icon that is to be displayed when the cursor is moved onto the icon.

`icondisable="`*icon-storage-path*`";`

Specifies the full path of the icon that is to be displayed when the corresponding program cannot be started.

`execute_id="`*program-identifier*`";`

Specifies an identifier for the program that is to be started. You can specify from 1 to 32 alphanumeric characters. This character string must be unique within the definition file. The program identifier specified in this parameter must be the same as a program identifier that is specified in the start program definition file (`!JP1_CS_APP0.conf`). For details about the start program definition file (`!JP1_CS_APP0.conf`), see *Start program definition file (!JP1_CS_APP0.conf)* in *Chapter 2. Definition Files*.

`arguments="`*arguments*`";`

Specifies arguments for the program to be started (start path) that is defined in the start program definition file (`!JP1_CS_APP0.conf`). For details about the start program definition file (`!JP1_CS_APP0.conf`), see *Start program definition file (!JP1_CS_APP0.conf)* in *Chapter 2. Definition Files*.

Example definition

```
#------------------------------------------------------------
# Definition changed by 07-00.
@define-block type="function-tree-def";
id="tool_notepad";
name="Notepad";
iconstandard="%SOV_INSTALL_PATH%\image\sovtool\blank_standard.gif";
icondown="%SOV_INSTALL_PATH%\image\sovtool\blank_down.gif";
iconrollover="%SOV_INSTALL_PATH%\image\sovtool\blank_over.gif";
icondisable="%SOV_INSTALL_PATH%\image\sovtool\blank_disable.gif";
execute_id="app_notepad";
arguments="C:\test.txt";
@define-block-end;
#------------------------------------------------------------
```

Configuration file for monitoring tree

Format

```
TREE:BUILD=value;ID=value;[DATE=generation-date-and-time;]CSV_VER=09000000;M
SCOPE=ON (linefeed)
OBJ:monitoring-node-name#, NID:monitoring-node-ID#, ICO:icon-name, TYPE:monit
oring-node-type, CLASS:monitoring-object-type, STA:status-ID, CHDT:status-up
date-time, OBS:monitoring-status, STD:basic-information (attribute-name-1=at
tribute-name-1#), BKIMG=background-image-file-name, POT:X=X-coordinate;Y=Y-co
ordinate;Z=Z-coordinate, CON:NAME=status-change-condition-name#, STA=change-s
tatus-ID, CID=common-condition-ID;common-condition-information, GCON:NAME=st
atus-change-condition-name#, STA=change-status-ID, CSTA=child-node-status-ID
, NUM>=child-node-count, RATIO>=child-node-ratio, (individual-condition-name
==individual-condition-value#), EVE:STA=status-ID, RES:JP1-resource-group-nam
e, OWN:monitoring-node-owner's-name, OPE:list-of-operation-items (linefeed)
          :
```

Legend:

(linefeed): Location of a linefeed

#: Item that can be edited (all other items cannot be edited)

File

Any file (configuration file for monitoring tree)

Storage directory

Any folder

Description

This file defines the configuration of the monitoring tree that is displayed in the Monitoring Tree window.

By editing the configuration file for the monitoring tree, you can change the information that is displayed in the monitoring tree, such as the names of monitoring nodes and attribute values of basic information. To create a configuration file for monitoring tree, save the tree configuration locally from the Monitoring Tree window or Monitoring Tree (Editing) window. Do not create a configuration file for monitoring tree by any other method. When you edit the configuration file for monitoring tree, make sure that you do not edit any values other than those described below.

If you have updated an uneditable value by mistake and a backup of the configuration file for monitoring tree is available, use the backup file to update the configuration file for monitoring tree again. If no backup file is available, use the `jcsdbsetup` or `jcsdbimport` command to set up the monitoring object database again.

It is preferable that you use the Monitoring Tree (Editing) window to edit the monitoring tree, unless otherwise necessary.

To use two-byte characters, standardize the character encoding as MS932. No custom characters can be used. Do not enter an escape character.

When the definitions are applied

The definition takes effect when it is applied to JP1/IM - Manager after this definition file has been opened in the Monitoring Tree (Editing) window.

Information that is specified

`TREE`

The following parameters contained in `TREE` cannot be changed.

`BUILD=`*value*

value displays the tree generation number. This parameter value is changed by updating at the server.

`ID=`*value*

value displays the tree ID.

`DATE=`*generation-date-and-time*

generation-date-and-time displays the date and time the tree was generated. This parameter's value is updated when a server update is performed and when the status of a monitoring node changes.

`CSV_VER=09000000`

This is the CSV file format version. The value might be different depending on the version of JP1/IM - Manager.

`MSCOPE={ON | OFF}`

Displays whether the monitoring range settings are enabled or disabled. `ON` means that the monitoring range settings are enabled.

`OBJ:`*monitoring-node-name*

Displays the name of a monitoring node that is to be displayed in the monitoring tree. The user can change this information. You can specify a character string with a maximum of 255 bytes. Specifiable characters are one-byte alphanumeric characters and two-byte characters (except custom characters). If you use a semicolon (`;`) in the monitoring node name, enter two consecutive semicolons.

If the monitoring node name contains a comma (`,`), enclose the entire `OBJ` item in double-quotation marks (`"`).

Example:

To specify `"monitoring,node"` as the name of a monitoring node, specify as follows:

```
"OBJ:monitoring,node"
```

If you enclose the monitoring node name in double-quotation marks (`"`), you must enclose the monitoring node name in another set of double-quotation marks and then also enclose the entire `OBJ` item in double-quotation marks.

Example:

To specify `"monitoring node"` as the monitoring node name, specify as follows:

```
"OBJ:""monitoring node"""
```

`NID:`*monitoring-node-ID*

Displays the ID (8 hexadecimal characters) of the monitoring node that is to be displayed in the monitoring tree. The user can change this information.

Make sure that each monitoring node ID is unique. Specify a value in the range from `00000001` to `7FFFFFFF`.

`ICO:`*icon-name*

Displays a maximum of three icon names for the monitoring node, separated by the semicolon (`;`).

This parameter cannot be changed.

`TYPE:`*monitoring-node-type*

Displays the ID that identifies the monitoring group, monitoring object, and virtual root node. This parameter cannot be changed.

`CLASS:`*monitoring-object-type*

Displays the type of monitoring node. This parameter cannot be changed.

STA:*status-ID*

Displays the ID that indicates the status of the monitoring node. This parameter cannot be changed.

CHDT:*status-update-time*

Displays the time the status of the monitoring node was updated. This parameter cannot be changed.

OBS:*monitoring-status*

Displays the monitoring status of the monitoring node. This parameter cannot be changed.

STD:*attribute-name=attribute-value*

Displays the attribute name and attribute value when basic information has been defined for the monitoring node. If multiple basic information items are specified, the items are separated by the semicolon (;).

You can change only *attribute-value*. You can specify a maximum of 1,023 bytes# of characters for the attribute value. If you use a semicolon (;) in the attribute value, enter two consecutive semicolons.

#: The total length of the field is a maximum of 1,280 bytes (for example, if five basic information items are set, the total length of all five attribute values must be no greater than 1,280 bytes).

If the attribute value contains a comma (,), enclose the entire STD item in double-quotation marks (").

Example:

To specify attribute,value as the attribute value, specify as follows:

"STD:*attribute-name*=attribute,value"

If you enclose the attribute value in double-quotation marks ("), you must enclose the attribute value in another set of double-quotation marks and then also enclose the entire STD item in double-quotation marks.

Example:

To specify "attribute value" as the attribute value, specify as follows:

"STD:*attribute-name*=""attribute value"""

BKIMG=*background-image-file-name*

Displays the name of the background image file that is set in the Visual Monitoring (Editing) window or that is set when the map is displayed in the Monitoring Tree (Editing) window. This parameter cannot be changed.

POT:X=*X-coordinate*;Y=*Y-coordinate*;Z=*Z-coordinate*

Displays the icon location information (coordinates) that is set in the Visual Monitoring (Editing) window or that is set when the map is displayed in the Monitoring Tree (Editing) window. This parameter cannot be changed.

CON

CON includes the parameters shown below. Note that if the value of TYPE is 1 (monitoring group), the CON parameter is not displayed.

NAME=*status-change-condition-name*

Displays the status change condition name. The user can change this information. Specifiable characters are one-byte alphanumeric characters and two-byte characters (except custom characters). None of the following characters can be used: * " ' \ : ; | = + ? < . >. If the line contains more than one NAME parameter, the same status change condition name cannot be used more than once on that line.

If the status change condition name contains a comma (,), enclose the entire CON item in double-quotation marks (").

Example:

To specify "status change,condition name" as the status change condition name, specify as follows:

```
"CON:NAME=status change,condition name;
STA=700;
individual condition name==individual condition value"
```

STA=*change-status-ID*

Displays the change status ID. This parameter cannot be changed.

CID=*common-condition-ID*;*common-condition-information*

Displays the common condition ID and the common condition information. For the common condition information, the common conditions that have been set in the Status-Change Condition Settings window, such as the ID and information needed by the system for management purposes, are displayed with the items separated by the semicolon (;). This parameter cannot be changed.

GCON

GCON includes the parameters described below.

Note that the GCON parameter is not displayed if the value of TYPE is 2 (monitoring object) or if no status change condition has been set for the monitoring group.

NAME=*status-change-condition-name*

Displays the status change condition name. The user can change this information. Specifiable characters are one-byte alphanumeric characters and two-byte characters (except custom characters). None of the following characters can be specified: * " ' \ : ; | = + ? < . >. If the line contains more than one NAME parameter, the same status change condition name cannot be used more than once on that line.

If the status change condition name contains a comma (,), enclose the entire GCON item in double-quotation marks (").

STA=*change-status-ID*

Displays the change status ID. This parameter cannot be changed.

CSTA=*child-node-status-ID*

Displays the status IDs of child nodes. This parameter cannot be changed.

NUM>=*child-nodes-count*

Displays the number of child nodes. This parameter cannot be changed. This parameter and the RATIO parameter are mutually exclusive.

RATIO>=*child-node-ratio*

Displays the ratio of child nodes. This parameter cannot be changed. This parameter and the NUM parameter are mutually exclusive.

individual-condition-name==*individual-condition-value*

Displays an individual condition if it has been set in the Status-Change Condition Settings window. If multiple individual conditions have been specified, they are separated by the semicolon (;). You can change only *individual-condition-value*. The == part depends on the setting in the GUI as shown below; do not change this part.

```
== (same as)
!= (not same as)
^= (starts with)
>= (includes)
<= (does not include)
*= (regular expression)
+= (host name comparison)
```

For *individual-condition-value*, you can specify a maximum of 1,023 bytes# of characters. If you use a semicolon (;) in an individual condition value, enter two consecutive semicolons.

#: The total length of the field is a maximum of 1,280 bytes (for example, if five individual conditions are set, the total length of all five condition values must be no greater than 1,280 bytes).

If an individual condition value contains a comma (`,`), enclose the entire `CON` item in double-quotation marks (`"`).

Example:

To specify `"individual,condition value"` as the individual condition value, specify as follows:

```
"CON:NAME=status change condition name;
STA=700;
individual condition name==individual,condition value"
```

If you enclose the individual condition value in double-quotation marks (`"`), you must enclose the individual condition value in another set of double-quotation marks and then also enclose the entire `CON` item in double-quotation marks.

Example:

To specify `""individual condition value""` as the individual condition value, specify as follows:

```
"CON:NAME=status change condition name,;
STA=700;
individual condition name==""individual condition name"""
```

`EVE:STA=`*status-ID*

Displays the status ID that was set in the event generation condition. This parameter cannot be changed.

`RES:`*JP1-resource-group-name*

Displays the JP1 resource group name of the monitoring node. This parameter cannot be changed.

`OWN:`*monitoring-node-owner's-name*

Displays the name of the monitoring node owner. This parameter cannot be changed.

`OPE:`*list-of-operation-items*

Displays a list of operation items that the login user has for the monitoring node. This parameter cannot be changed.

Note

- If you change the monitoring node ID, there may be adverse effects on the Visual Monitoring window. This is because the monitoring node IDs are used to manage the monitoring nodes that are displayed in the Monitoring Tree window and the Visual Monitoring window.

  If you have changed a monitoring node ID, make sure that there are no problems on the Visual Monitoring window.

System profile of Central Scope (jcs_sysprofile_xxx.def)

Format

```
DESC_VERSION=1#1
[SystemProfile]
  FrameVisible={true | false}
  Movable={true | false}
[DisplayColor]
    :
  [ColorItem]#2
    Status=monitoring-node-status-identifier
    Name=monitoring-node-status-name
    [Label]
      R=value
      G=value
      B=value
      A=value
    [END]
    [TEXT]
      R=value
      G=value
      B=value
    [End]
  [End]
      :
[End]
[DisplayLamp]
  Status=monitoring-node-status-identifier
[End]
[End]
```

#1: Do not change `DESC_VERSION=1`.

#2: Do not change the values of `Status` and `Name` between `[ColorItem]` and `[End]`.

File

For the system profile of Central Scope (`jcs_sysprofile_`*`xxx`*`.def`), the file to edit varies depending on the language in which JP1/IM runs. The following table explains the relation between the language code where JP1/IM runs and the system profile of Central Scope to edit.

Table 2–82: Language codes where JP1/IM runs and the system profile of Central Scope

OS	Language type	Language encoding supported by JP1/IM	Definition file
Windows	Japanese		`jcs_sysprofile_sjis.def` (System profile (Central Scope))
			`jcs_sysprofile_sjis.def.model` (Model file for the system profile (Central Scope))
	English		`jcs_sysprofile.def` (System profile (Central Scope))
			`jcs_sysprofile.def.model` (Model file for the system profile (Central Scope))

OS	Language type	Language encoding supported by JP1/IM	Definition file
	Chinese		jcs_sysprofile_GB18030.def (System profile (Central Scope))
			jcs_sysprofile_GB18030.def.model (Model file for the system profile (Central Scope))
UNIX#	Japanese	Shift-JIS encoding	jcs_sysprofile_sjis.def (System profile (Central Scope))
			jcs_sysprofile_sjis.def.model (Model file for the system profile (Central Scope))
		EUC encoding	jcs_sysprofile_euc.def (System profile (Central Scope))
			jcs_sysprofile_euc.def.model (Model file for the system profile (Central Scope))
		UTF-8 encoding	jcs_sysprofile_UTF-8.def (System profile (Central Scope))
			jcs_sysprofile_UTF-8.def.model (Model file for the system profile (Central Scope))
	English		jcs_sysprofile.def (System profile (Central Scope))
			jcs_sysprofile.def.model (Model file for the system profile (Central Scope))
	Chinese	GB18030 encoding	jcs_sysprofile_GB18030.def (System profile (Central Scope))
			jcs_sysprofile_GB18030.def.model (Model file for the system profile (Central Scope))

#

Only files of languages supported by the OS are included.

Use the system profile of Central Scope corresponding to the language code (jcs_sysprofile_*xxx*.def).

Storage directory

In Windows

For a physical host:

Scope-path\conf

For a logical host:

shared-folder\jp1scope\conf

In UNIX

For a physical host:

/etc/opt/jp1scope/conf

For a logical host:

shared-directory/jp1scope/conf

Description

Common definition information for the Central Scope viewer. The contents of this definition file are applied to the following windows:

- Monitoring Tree window

- Visual Monitoring window

When the definitions are applied

When you log in to Central Console, the definition takes effect. However, if you log in to Central Scope from the Event Console window, you must restart the Event Console window after editing the definition file, and then log in to Central Scope.

Information that is specified

`DESC_VERSION=1`

Indicates the system profile format version.

Do not change this value. If you do so, Central Scope Viewer might not operate correctly.

`[SystemProfile]` to `[End]`

Indicates the definition start tag and definition end tag for the system profile.

`FrameVisible={true | false}`

Specifies whether to display the monitoring node name and the space around an icon. You can specify either `true` or `false`. The value is not case sensitive. Write this parameter between `SystemProfile` and `End`.

If you specify `true`, the monitoring node name and the space around an icon are displayed. If you specify `false`, they are not displayed.

If you omit this parameter, or specify a value other than `true` or `false`, `true` is assumed.

If you upgrade JP1/IM - Manager from version 10-10 or earlier, this parameter is not set for the system profile of the logical host. To specify this parameter, add the description.

`Movable={true | false}`

Specifies whether to allow drag and drop operations for the monitoring node icon in the map display of the Monitoring Tree window, and the Visual Monitoring window. You can specify either `true` or `false`. The value is not case sensitive. Write this parameter between `SystemProfile` and `End`.

If you specify `true`, you can move the monitoring node icon. If you specify `false`, you cannot move it.

If you omit this parameter, or specify a value other than `true` or `false`, `true` is assumed.

If you upgrade JP1/IM - Manager from version 10-10 or earlier, this parameter is not set for the system profile of the logical host. To specify this parameter, add the description.

`[DisplayColor]` to `[End]`

Write a definition block to define the monitoring node status between `DisplayColor` and `End`. Write only one definition block between `SystemProfile` and `End`.

`[ColorItem]` to `[End]`

Write the status identifier, status name, and parameter to define the status color, and definition block between `[ColorItem]` and `[End]`. Write this definition block between `[DisplayColor]` and `[End]` for each status.

`Status=`*monitoring-node-status-identifier*

Specify the status identifier. Write this parameter between `[ColorItem]` and `[End]`. Do not change this value. If you do so, Central Scope Viewer might not operate correctly.

`Name=`*monitoring-node-status-name*

Specify the status name. Write this parameter between `[ColorItem]` and `[End]`. Do not change this value. If you do so, Central Scope Viewer might not operate correctly.

`[Label]` to `[End]`

Write parameters to specify the monitoring node status color, and whether to make the monitoring node color transparent between `[Label]` and `[End]`. When the monitoring node status changes, the color changes to the one corresponding to the new status specified between `[Label]` and `[End]`. Write this definition block only once between `[ColorItem]` and `[End]`.

`R=`*value*, `G=`*value*, `B=`*value*

Specifies the status color of the monitoring node by using the RGB value. Write this parameter between `[Label]` and `[End]`. You can specify an integer from 0 to 255.

If you omit this parameter, specify an integer less than 0, or specify a value other than an integer, 0 is assumed. If you specify a value greater than 255, 255 is assumed.

`A=`*value*

Specify whether to make the monitoring node status color transparent. Write this parameter between `[Label]` and `[End]`. If the `FrameVisible` parameter is not specified, and `true` is specified for the `FrameVisible` parameter, the status color cannot be transparent regardless the value specified for `A`. You can specify an integer from 0 to 255. The smaller the value you specify, the higher the transparent ratio is. If you specify 0, the status color is completely transparent. If you specify 255, the status color is not transparent.

If you omit this parameter, or specify a value that cannot be specified, 255 is assumed.

`[TEXT]` to `[End]`

Write parameters to specify the text color of the monitoring node name between `[TEXT]` and `[End]`. When the monitoring node status changes, the monitoring node name text color changes to the one corresponding to the new status specified between `[TEXT]` and `[End]`. Write this definition block only once between `[ColorItem]` and `[End]`.

`R=`*value*, `G=`*value*, `B=`*value*

Specifies the monitoring node name text color by using the RGB values. Write these parameters between `[TEXT]` and `[End]`. You can specify an integer from 0 to 255.

If you omit this parameter, specify a value less than 0, or specify a non-integer value, 0 is assumed. If you specify a value greater than 255, 255 is assumed. In the initial status after installation, 0 is specified for all of R, G, and B values.

`[DisplayLamp]` to `[End]`

Specify parameters used to specify the status when an alarm lamp turns on. When the highest monitoring node status changes, if the status identifier specified for the new status is greater than the value specified between `[DisplayLamp]` and `[End]`, the applicable alarm lamp turns on. You must write this definition block between `[SystemProfile]` and `[End]`.

`Status=`*monitoring-node-status-identifier*

Specify the status when an alarm lamp turns on. Write this parameter between `[DisplayLamp]` and `[End]`. You can specify a decimal integer from -2,147,483,648 to 2,147,483,647.

If you omit this parameter, or specify a value that cannot be specified, `0` is assumed. If the status indicator specified for the highest monitoring node status is greater than the value specified for this parameter, an alarm lump turns on. The following table explains the correspondences between the values specified for this parameter and the statuses when the alarm lamp turns on.

Table 2–83: Correspondence between the specified values and the statuses when the alarm lamp turns on

Specified value	Status when the alarm lump turns on
`-2,147,483,648` to `100`	Initial, debug, normal, warning, error, critical, alert, and emergency
`101` to `200`	Debug, normal, warning, error, critical, alert, and emergency
`201` to `300`	Normal, warning, error, critical, alert, and emergency
`301` to `400`	Warning, error, critical, alert, and emergency

Specified value	Status when the alarm lump turns on
401 to 500	Error, critical, alert, and emergency
501 to 600	Critical, alert, and emergency
601 to 700	Alert, and emergency
701 to 800	Emergency
801 to 2,147,483,648	Does not turn on

We recommend you specify 200, 300, 400, 500, 600, 700, or 800.

Notes

- The setting item name is case sensitive.
- Specify a value for each item immediately after the equal sign (=). If you add a space or a tag, the value cannot be recognized.
- If the start tag is unintentionally deleted, the file format invalid message (KAVB7303-E) is output, and the operation of JP1/IM - View stops. Also, if the tag is unintentionally changed, the definition is not recognized.
- If the end tag is unintentionally changed or deleted, the file format invalid message (KAVB7303-E) is output, and the operation of JP1/IM - View stops.
- If you edit the system profile of Central Scope (jcs_sysprofile_*xxx*.def), the changes are not applied to the Monitoring Tree (Editing) and Visual Monitoring (Editing) windows. If you want to change settings of these windows, edit the system profile of the Central Scope viewer (system.conf).

System profile of the Central Scope viewer (system.conf)

Format

```
DESC_VERSION=1
[SystemProfile]
  FrameVisible={true | false}
 [DisplayColor]
     :
  [ColorItem]
    Status=monitoring-node-status-identifier
    Name=monitoring-node-status-name
    [Label]
      R=value
      G=value
      B=value
      A=value
    [END]
    [TEXT]
      R=value
      G=value
      B=value
    [End]
  [End]
      :
[End]

[End]
```

File

`system.conf` (System profile of the Central Scope viewer)

`system.conf.model` (Model file of the system profile of the Central Scope viewer)

Storage directory

For Japanese operating systems:
View-path`\conf\sovsystem\ja\`

For English operating systems:
View-path`\conf\sovsystem\en\`

For Chinese operating systems:
View-path`\conf\sovsystem\zh\`

Description

Common definition information for Central Scope viewer. Contents of this definition file are applied to the following windows:

- Monitoring Tree (Editing) window
- Visual Monitoring (Editing) window

When the definitions are applied

The definitions are applied when the Monitoring Tree (Editing) window or the Visual Monitoring (Editing) window is displayed.

Information that is specified

`Movable` cannot be specified. All other specifications are the same as the system profile of Central Scope (`jcs_sysprofile_`*`xxx`*`.def`). For details, see *System profile of Central Scope (jcs_sysprofile_xxx.def)* in *Chapter 2. Definition Files*.

Notes

Notes specific to the system profile of the Central Scope viewer (`system.conf`) are provided here. For notes on other issues, see *System profile of Central Scope (jcs_sysprofile_xxx.def)* in *Chapter 2. Definition Files*.

- The monitoring node in the Monitoring Tree (Editing) and Visual Monitoring (Editing) windows are always initial state. As a result, definitions for other statuses are not applied to the windows.
- If you edit the system profile of the Central Scope viewer (`system.conf`), the changes are not applied to the Monitoring Tree and Visual Monitoring windows. If you want to change settings for these windows, edit the system profile of Central Scope (`jcs_sysprofile_`*`xxx`*`.def`).

Performance report display definition file (performance.conf)

Format

```
# (JP1/PFM - Web Console URL)
[URL-of-JP1/PFM-Web-Console]
```

File

`performance.conf` (performance report display definition file)

`performance.conf.model` (model file for the performance report display definition file)

Storage directory

In Windows

Physical host:

Console-path`\conf\console\performance`

Logical host:

shared-folder`\jp1cons\conf\console\performance`

In UNIX

Physical host:

`/etc/opt/jp1cons/conf/console/performance`

Logical host:

shared-directory`/jp1cons/conf/console/performance`

Description

This file defines the function for displaying the performance report of the host that issued an event. The file defines the URL of the connection-target instance of JP1/PFM - Web Console.

When the definitions are applied

The settings in the performance report display definition file take effect when you log in to JP1/IM - Manager in JP1/IM - View after the `jco_spmd_reload` command has been executed or when you log in to JP1/IM - Manager in JP1/IM - View after JP1/IM - Manager has been restarted.

Information that is specified

- Tab characters, leading single-byte spaces, and trailing single-byte spaces are ignored.
- Lines consisting of only single-byte spaces or tab characters and null lines (lines that contain only an end-of-line code) are ignored, and processing continues.
- A line beginning with a hash mark (`#`) is treated as a comment.

`[`*URL-of-JP1/PFM-Web-Console*`]`

Specify the URL of the connection-target instance of JP1/PFM - Web Console by using single-byte alphanumeric characters and symbols.

For details about the JP1/PFM - Web Console URL, see the applicable JP1/PFM manual.

Notes

For the character encoding of the file, use the same character encoding set for the manager.

Operation definition file for IM Configuration Management - View (jcfview.conf)

Format

```
jcfview.login.host.max=maximum-number-of-recorded-hosts
jcfview.login.user.max={0|1}
jcfview.screen.history.enable={0|1}
jcfview.response.wait.time=server-response-wait-timeout-period
jcfview.imconfigreflect.response.wait.time=response-wait-timeout-period-for-
reflection-of-system hierarchy
jcfview.screen.title.logininfo.enable={0|1}
```

File

`jcfview.conf` (operation definition file for IM Configuration Management - View)

`jcfview.conf.model` (model file for the operation definition file for IM Configuration Management - View

Storage directory

View-path`\conf\jcfview\`

Description

This file specifies the operation of IM Configuration Management - View.

When the definitions are applied

The definition takes effect when IM Configuration Management - View starts.

Information that is specified

`jcfview.login.host.max=`*maximum-number-of-recorded-hosts*

Specifies as a decimal value the maximum number of hosts that have logged in successfully. Permitted values are from `0` to `20`. The default is `5`.

`jcfview.login.user.max={0|1}`

Specifies whether to display the name of the JP1 user who logged in previously in the **User name** text box of the Login window. If `1` is specified, the name of the user who logged in previously is displayed. If `0` is specified, the name of the user is hidden. If you omit this parameter, or if you specify a value other than `0` or `1`, `1` is assumed. The default is `1`.

`jcfview.screen.history.enable={0|1}`

Specifies whether the function that inherits the display position and size of the IM Configuration Management - View window, as well as the selection status of the displayed buttons that were in use the last time the screen was open, is to be used. This setting applies to the IM Configuration Management window, the Edit Agent Configuration window, the Edit Remote Monitoring Configuration window, and the Display/Edit Profiles window.

The permitted values are as follows:

- `0`: Do not use the window display settings history function.
- `1`: Use the window display settings history function (default value).

Note that if you specify `0` and then start IM - View, all the window display settings history files will be deleted.

`jcfview.response.wait.time=`*server-response-wait-timeout-period*

Specifies in decimal notation the timeout period for waiting for a response when applying the hierarchy configuration (IM configuration) to the system.

The permitted value range is from 60,000 to 3,600,000; the default is 1,800,000. If the specified value is less than the minimum value, greater than the maximum value, invalid, or undefined, the default value is used.

When a timeout occurs, the `KNAN20105-E` message is displayed. If the `KNAN20105-E` message is issued frequently, we recommend that you revise the timeout setting.

`jcfview.imconfigreflect.response.wait.time=`*response-wait-timeout-period-for-updating-system-hierarchy*

Specifies in milliseconds in decimal notation the timeout period for waiting for the system hierarchy to be applied. The permitted value range is from 60,000 to 36,000,000; the default is 18,000,000. If the specified value is less than the minimum value, greater than the maximum value, invalid, or undefined, the default value is used.

When a timeout occurs, the `KNAN20105-E` message is displayed. If the `KNAN20105-E` message is issued frequently, revise the timeout setting.

`jcfview.screen.title.logininfo.enable={0|1}`

You can prevent the name of the logged-in JP1 user from being displayed in the title of the IM Configuration Management window, the Edit Agent Configuration window, the Edit Remote Monitoring Configuration window, and the Display/Edit Profiles window. When `1` is specified, the name of the logged in JP1 user is displayed. When `0` is specified, the name of the user is hidden. If you omit this parameter, or if you specify a value other than `0` or `1`, `1` is assumed. The default is `1`.

Example definition

```
jcfview.login.host.max=5
jcfview.login.user.max=1
jcfview.screen.history.enable=1
jcfview.response.wait.time=1800000
jcfview.imconfigreflect.response.wait.time=18000000
jcfview.screen.title.logininfo.enable=1
```

Apply-IM-configuration-method definition file (jp1cf_applyconfig.conf)

Format

```
[logical-host-name\JP1CONFIG]
"APPLY_CONFIG_TYPE"=dword:{00000000 | 00000001}
```

File

`jp1cf_applyconfig.conf` (file that sets the application method of IM configuration)

Storage directory

In Windows

For a physical host:

Manager-path`\conf\imcf\`

For a logical host:

shared-folder`\JP1IMM\conf\imcf\`

In UNIX

For a physical host:

Physical host: `/etc/opt/jp1imm/conf/imcf/`

For a logical host:

Logical host: *shared-directory*`/jp1imm/conf/imcf/`

Description

This file defines how to apply the system hierarchy.

The methods for applying the agent configurations include the differential distribution method, the batch distribution method (with the deletion of configuration information), and the batch distribution method (without the deletion of configuration information).

When the condition below is met, you can use the apply-IM-configuration-method definition file to switch between the batch distribution method (with the deletion of configuration information) and the batch distribution method (without the deletion of configuration information):

- The differential distribution functionality is disabled in the JP1/Base settings for distributing configuration definition information, and the function for restricting the viewing of and operations on business groups is disabled.

For details about how to apply the system hierarchy, see *8.2.6 Applying the system hierarchy* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

When the definitions are applied

After the `jbssetcnf` command is executed to apply the definitions to the JP1 common definition information, the settings are applied when JP1/IM - Manager is started or restarted, or when the file is reloaded by using the `jco_spmd_reload` command.

Information that is specified

[*logical-host-name*`\JP1CONFIG]`

Indicates the key name of the application method of IM configuration.

For the physical host, specify `JP1_DEFAULT` for *logical-host-name*. For a logical host, specify its name for *logical-host-name*.

`"APPLY_CONFIG_TYPE"=dword:{00000000 | 00000001}`

Specify the method for applying the system hierarchy.

- 00000000

  Specify this value to use the batch distribution method (with the deletion of configuration information) to apply the system hierarchy. Applies the system hierarchy configuration after deletion. This item is set by default.

- 00000001

  Specify this value to use the batch distribution method (without the deletion of configuration information) apply the system hierarchy. Applies the system hierarchy configuration without deleting it.

If the value is invalid or if the common definition has not been set, the default value is assumed.

Example definition

```
[JP1_DEFAULT\JP1CONFIG]
"APPLY_CONFIG_TYPE"=dword:00000001
```

Host input information file (host_input_data.csv)

Format

```
product-name;file-format-version;character-encoding
Host_name,IPAddress,Host_list,Comment,Host_type,Running_host_name,Standby_ho
st_name,VMM_host_name,Virtual_manager_type,Username,Password,Domain_name,Con
nection_type,Virtual_host_manager,Remote_connection_type,Authentication_sect
ion,Port_number,SSH_private_key_path
host-name,IP-address,list-of-host-names,comment,host-type,executing-host,sta
ndby-host,VMM-host,virtulization-management-type,user-name,password,domain-n
ame,communication-type,virtulization-management-former-host-name,remote-comm
unication-type,authentication-information-section, port-number, private-key-
path
```

File

`host_input_data.csv` (host input information file)

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file is the export file for host input information related to hosts managed by IM Configuration Management. You can edit and import this file.

When the definitions are applied

The definitions are applied when the file is imported by using the `jcfimport` command.

Information that is specified

The following table describes the host information to be output to the host input information file.

Table 2–84: Host information to be exported (host input information file)

Line	Output item	Output value
Line 1 (header information)	Product name	`JP1/IM-CF`
	File format version	File format version. For example, if the JP1/IM - Manager version is 10-50, `101000` is output.
	Character encoding	Character encoding. The value depends on the LANG environment variable setting of the manager. For details, see *Table 2-85 Character encoding of files*.
Line 2 (header information)	Host name	`Host_name`
	IP address	`IPAddress`
	List of host names	`Host_list`

Line	Output item	Output value
	Comment	`Comment`
	Host type	`Host_type`
	Executing host	`Running_host_name`
	Standby host	`Standby_host_name`
	VMM host	`VMM_host_name`
	Virtualization management type	`Virtual_manager_type`
	User name	`Username`
	Password	`Password`
	Domain name	`Domain_name`
	Communication type	`Connection_type`
	Virtualization management former host name	`Virtual_host_manager`
	Remote communication type	`Remote_connection_type`
	Authentication information section	`Authentication_section`
	Port number	`Port_number`
	Private key path	`SSH_private_key_path`
Line 3 and subsequent lines	Host name	Name of a host registered in the system hierarchy configuration
	IP address	IP address of a host registered in the system hierarchy configuration (When there are multiple IP addresses, separate them by a comma (`,`), and enclose all IP addresses in double-quotation marks (`"`)).
	List of host names	List of host names registered on a host (When there are multiple lists, separate them by a comma (`,`), and enclose all lists in double-quotation marks (`"`)).
	Comment	Comment registered on a host
	Host type	Type of host (`physical`, `logical`, `virtual`, `unknown`)
	Executing host	Name of the host used as the executing host
	Standby host	Name of the host used the standby host (When there are multiple standby host names, separate them by a comma (`,`), and enclose all standby host names in double-quotation marks (`"`)).
	VMM host	Name of the host on which the virtual machine monitor is running
	Virtualization management type	Type of virtualization management (`vCenter`, `JP1/SC/CM`, `SCVMM`, `HCSM`, `ESX`#1, `Hyper-V`, `KVM`, `Virtage`#2)
	User name	User name
	Password	Password information is not output.
	Domain name	Domain name of the host on which the virtual machine monitor is running.
	Communication type	Communication type (`http`, `https`, `ssh`)
	Virtualization management former host name	Host name registered on a host

Line	Output item	Output value
	Remote communication type	Communication type to be output for remote monitoring (`disable`, `ssh`, `wmi`)
	Authentication information section	Authentication information to be output for remote monitoring (`common`, `host`, blank)
	Port number	Number of the port used for communication
	Private key path	Absolute path of the private key file to be used for SSH connection

#1: `ESX` indicates VMware ESX.

#2: `Virtage` indicates the Hitachi Compute Blade logical partitioning feature.

Table 2–85: Character encoding of files

OS	Format of the LANG environment variable	Character encoding to be converted
Windows	--	Japanese OS: MS932
		English OS: C (ISO-8859-1)
		Chinese OS: GB18030
Linux	`ja_JP.UTF-8` or `ja_JP.utf8`	Japanese OS: UTF-8
	`ja_JP.sjis` or `ja_JP.SJIS`#	Japanese OS: Shift_JIS
	`C`	English OS: C (ISO-8859-1)
	`zh_CN.gb18030`	Chinese OS: GB18030
--	Other than above	UTF-8

Legend:

--: Not applicable

#: Valid only when the OS is SUSE Linux.

Output example

```
JP1/IM-CF;101000;MS932,,,,,,,,,,,,,,,,
Host_name,IPAddress,Host_list,Comment,Host_type,Running_host_name,Standby_ho
st_name,VMM_host_name, Virtual_manager_type,Username,Password, Domain_name,
Connection_type,Virtual_host_manager,Remote_connection_type,Authentication_s
ection, Port_number, SSH_private_key_path
infch05340,192.168.105.251,infch05340.supp528,,physical,,,,,,,,,,disable,,
infch05356,192.168.105.193,infch05356,,physical,,,,,,,,,,disable,,
infch02272,192.168.105.84,infch02272,,physical,,,,KVM,,,,,,disable,22,<ssh_p
rivate_key_path>
```

Collected host information file (host_collect_data.csv)

Format

```
product-name;file-format-version;character-encoding
Real_host_name,OS_name,JP1_product_name,JP1_product_id,JP1_product_version,I
nstall_path,Conf_dir,Date,Total_time,Host_name,Virtual_manager_type,Virtual_
manager_version
real-host-name,OS-name,product-name,product-model-name,version,installation-
path,environment-setting-file-storage-folder,update-date/time,update-date/ti
me-GMT,host-name,virtualization-management-type,virtualization-product-versi
on
```

File

`host_collect_data.csv` (collected host information file)

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file is the export file for collected host information related to managed hosts of IM Configuration Management. This file cannot be edited or imported.

Information that is specified

The following table describes the host information to be output to the collected host information file.

Table 2–86: Host information to be exported (Collected host information file)

Line	Output item	Output value
Line 1 (header information)	Product name	`JP1/IM-CF`
	File format version	File format version. For example, if the JP1/IM - Manager version is 10-50, `101000` is output.
	Character encoding	Character encoding. The value depends on the LANG environment variable setting of the manager. For details, see *Table 2-85 Character encoding of files*.
Line 2 (header information)	Real host name	`Real_host_name`
	OS name	`OS_name`
	Product name	`JP1_product_name`
	Product model name	`JP1_product_id`
	Version	`JP1_product_version`
	Installation path	`Install_path`

Line	Output item	Output value
	Storage folder for the environment settings file	`Conf_dir`
	Update date/time	`Date`
	Update date/time (GMT)	`Total_time`
	Host name	`Host_name`
	Virtualization management type	`Virtual_manager_type`
	Virtualization product version	`Virtual_manager_version`
Line 3 and the subsequent lines	Real host name	Real host name of a host
	OS name	Name of the OS running on a host
	Product name	Name of the product running on a host
	Product model name	Model name of a product
	Version	Product version
	Installation path	Installation path of a product
	Storage folder for the environment settings file	Folder in which the environment setting file of a product is stored
	Update date/time	*YYYY/MM/DD hh:mm:ss*
	Update date/time (GMT)	*YYYY/MM/DD hh:mm:ss* (GMT)#1
	Host name	Name of a host registered in the system hierarchy configuration
	Virtualization management type	Type of virtualization management (`vCenter`, `JP1/SC/CM`, `SCVMM`, `HCSM`, `ESX`#2, `Hyper-V`, `KVM`, `Virtage`#3)
	Virtualization product version#4	Version of a virtualization product. Virtualization configuration collection date/time is output as the update date/time.

#1: When virtualization software and virtualization environment management software are used, the virtualization configuration collection date/time is output.

#2: ESX indicates VMware ESX.

#3: Virtage indicates the Hitachi Compute Blade logical partitioning feature.

#4: If the virtualization management type is HCSM, the version of an external connection interface for HCSM is displayed. For this reason, the displayed version and the actual version for HCSM might be different. Furthermore, if you obtain virtualization configuration information from HCSM, the version number is not displayed for a host whose virtualization management type is Hitachi Compute Blade logical partitioning feature.

Output example

```
JP1/IM-CF;101000;UTF-8,,,,,,,,,,,
Real_host_name,OS_name,JP1_product_name,JP1_product_id,JP1_product_version,I
nstall_path,Conf_dir,Date,Total_time,Host_name,Virtual_manager_type,Virtual_
manager_version
jp1_bs1,Windows,JP1/Base,P-242C-6L94,0900,C:\Program Files\Hitachi\JP1Base,C
:\Program Files\Hitachi\JP1Base\conf,2009/11/28 10:45:20,1205115658437,jp1-b
s1,,
jp1-bs2,Windows, , , , , ,2009/11/28 10:45:20,1205115658437,jp1-bs2,ESX,3.5
jp1-bs3,Windows, , , , , ,2009/11/28 10:45:20,1205115658437,jp1-bs3,vCenter,
4.0
```

Profile management environment definition file (jp1cf_profile_manager.conf)

Format

```
[logical-host-name\JP1CONFIG\PROFILE_MANAGER\JP1BASE]
"LOGFILETRAP_AUTO_START_CONTROL"=dword:hexadecimal-number
"AGENT_PROFILE_UPDATE_NOTICE"=dword:hexadecimal-number
```

File

`jp1cf_profile_manager.conf` (profile management environment definition file)

`jp1cf_profile_manager.conf.model` (model file for the profile management environment definition file)

Storage directory

In Windows

Manager-path`\conf\imcf`

In UNIX

`/etc/opt/jp1imm/conf/imcf`

Description

This file defines information about the execution environment for the profile management function.

When the definitions are applied

The definition takes effect when JP1/IM - Manager is restarted after the `jbssetcnf` command is executed in JP1/Base to apply the definition in the profile management environment definition file to the JP1 common definition information.

Information that is specified

`[`*logical-host-name*`\JP1CONFIG\PROFILE_MANAGER\JP1BASE]`

Specify the key name of the profile management environment definition.

For *logical-host-name*, specify `JP1_DEFAULT` for a physical host and *logical-host-name* for a logical host.

`"LOGFILETRAP_AUTO_START_CONTROL"=dword:`*hexadecimal-number*

Specify whether to enable the use of the function for setting the automatic startup of log file traps in the Display/Edit Profiles window of JP1/IM - View. If this function is enabled, the **Start the process automatically when the log file trap service starts** check box is displayed in **Startup options**.

- `00000001`: Enable
- `00000000`: Disable

The default is `00000001` (enable).

`"AGENT_PROFILE_UPDATE_NOTICE"=dword:`*hexadecimal-number*

Specify whether to enable the use of the function that sends notifications indicating that agent profiles might have been updated when profiles are edited or applied in the Display/Edit Profiles window of JP1/IM - View.

- `00000001`: Enable
- `00000000`: Disable

The default is `00000001` (enable).

Remote log trap environment definition file (jp1cf_remote_logtrap.conf)

Format

```
[logical-host-name\JP1CONFIG\AGTLESS_MGR]
"MAX_COLLECT_EVENTLOG_DATA_SIZE"=dword:hexadecimal-number
"MAX_COLLECT_WIN_LOG_DATA_SIZE"=dword:hexadecimal-number
"MAX_COLLECT_UNIX_LOG_DATA_SIZE"=dword:hexadecimal-number
"START_OPTION"="warm" | "cold"
```

File

`jp1cf_remote_logtrap.conf` (remote log trap environment definition file)

`jp1cf_remote_logtrap.conf.model` (model file for the remote log trap environment definition file)

Storage directory

In Windows

Manager-path`\conf\imcf`

In UNIX

`/etc/opt/jp1imm/conf/imcf`

Description

This file defines an execution environment for the remote-monitoring log file trap function and the remote-monitoring event log trap function.

When the definitions are applied

In the common definition settings file, specify the remote log trap environment definition file as the argument for the `jbssetcnf` command. After that, the remote log trap environment definition file settings take effect when either of the following triggers occurs:

- When JP1/IM - Manager restarts
- When you perform a reload by executing the `jco_spmd_reload` command

Note that when this definition is applied, the total capacity of the logs that can be monitored by a single instance of JP1/IM - Manager is checked. If the capacity exceeds 10 MB, a `KNAN26143-W` warning message is output to the integrated trace log.

Information that is specified

`[`*logical-host-name*`\JP1CONFIG\AGTLESS_MGR]`

Specify the key name of the remote log trap environment definition.

For *logical-host-name*, specify `JP1_DEFAULT` for a physical host and *logical-host-name* for a logical host.

`"MAX_COLLECT_EVENTLOG_DATA_SIZE"=dword:`*hexadecimal-number*

Specifies in hexadecimal notation the maximum size of the event log that can be collected in one monitoring interval of the remote monitoring event log trap. You can specify any value in the range from `0x00002800` to `0x00032000` (10 KB to 200 KB). If this information is omitted, `0x00002800` (10 KB) is assumed.

"MAX_COLLECT_WIN_LOG_DATA_SIZE"=dword:*hexadecimal-number*

Specifies in hexadecimal notation the maximum size of the log that can be collected in one monitoring interval of the remote monitoring log file trap when the monitored host is Windows. You can specify any value in the range from 0x00002800 to 0x00032000 (10 KB to 200 KB). If this information is omitted, 0x00002800 (10 KB) is assumed.

"MAX_COLLECT_UNIX_LOG_DATA_SIZE"=dword:*hexadecimal-number*

Specifies in hexadecimal notation the maximum size of the log that can be collected in one monitoring interval of the remote monitoring log file trap when the monitored host is UNIX. You can specify any value in the range from 0x00002800 to 0x0000C800 (10 KB to 50 KB). If this information is omitted, 0x00002800 (10 KB) is assumed.

"START_OPTION"="warm" | "cold"

Specify whether logs that are output while remote monitoring is stopped are to be collected when remote monitoring resumes.

If "warm" is specified, logs that are output while remote monitoring is stopped will be collected.

If "cold" is specified, logs that are output while remote monitoring is stopped will not be collected.

If this information is omitted, "warm" is assumed.

Example definition

Example 1 (in Windows)

```
[JP1_DEFAULT\JP1CONFIG\AGTLESS_MGR]
"MAX_COLLECT_EVENTLOG_DATA_SIZE"=dword:00002800
"MAX_COLLECT_WIN_LOG_DATA_SIZE"=dword:00002800
"MAX_COLLECT_UNIX_LOG_DATA_SIZE"=dword:00002800
"START_OPTION"="warm"
```

Example 2 (In UNIX)

```
[JP1_DEFAULT\JP1CONFIG\AGTLESS_MGR]
"MAX_COLLECT_UNIX_LOG_DATA_SIZE"=dword:00002800
"START_OPTION"="warm"
```

If the manager host is a UNIX host and the managed host is a Windows host, remote monitoring cannot be performed. In such cases, if MAX_COLLECT_EVENTLOG_DATA_SIZE or MAX_COLLECT_WIN_LOG_DATA_SIZE is specified, it will be ignored.

Remote-monitoring log file-trap action definition file

Format

```
retry-times=number-of-retries
retry-interval=retry-interval
open-retry-times=number-of-retries
open-retry-interval=retry-interval
hold-count=number-of-held-JP1-events
keep-event={ OLD | NEW }
unset-extattr=attribute-suppressing-output
FILETYPE={ SEQ | SEQ2 | WRAP2 }
HEADLINE=number-of-header-lines
MARKSTR=[!]"regular-expression"
[!]"regular-expression-n"#
ACTDEF=[{EXIT}][event-level][event-ID][!]"regular-expression"
[!]"regular-expression-n"#
```

#: "*regular-expression-n*" indicates that multiple regular expressions are specified.

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines the actions for the remote monitoring log file trapping function. Its contents are referenced when the remote monitoring log file trapping function is started.

If you use UTF-8 as the encoding to save a file, save the file without attaching a BOM (byte order mark).

When the definitions are applied

The settings for the remote-monitoring log file-trap action definition file take effect at the following times:

- When a reload or restart operation is performed from the Display/Edit Profiles window

  For details about the Display/Edit Profiles window, see *5.9 Display/Edit Profiles window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

- When the `jcfallogstart` or `jcfallogreload` command is executed

  For details about the `jcfallogstart` command, see *jcfallogstart* in *Chapter 1. Commands*. For details about the `jcfallogreload` command, see *jcfallogreload* in *Chapter 1. Commands*.

- When JP1/IM - Manager is restarted

Information that is specified

`retry-times`

Specify a value from 0 to 86,400 for the number of retries to be attempted when a connection to an event service cannot be established due to a temporary communication failure. If this parameter is omitted, no retry operation is performed.

`retry-interval`

Specify a value from 1 to 600 (seconds) for the interval between retries to be performed when a connection to an event service cannot be established due to a communication failure. If this parameter is omitted, 10 seconds is assumed. This setting takes effect when the number of retries for connecting to an event service is set to one or a greater value. The retry interval is the interval between a failed attempt to connect to an event service and the next attempt. The time required for connection to an event service is not included. By combining `retry-times` and `retry-interval`, you can set a time equal to or longer than 24 hours, but if you do so and 24 hours or more passes after a retry attempt starts, retry processing stops.

`open-retry-times`

Specify a value from 1 to 3,600 as the number of retries to be performed if a log file cannot be read, or connection to the monitored host cannot be established. If this parameter is omitted, `1` is assumed. If the specified number of retries is exceeded, monitoring of the log file is stopped.

`open-retry-interval`

Specify a value from 3 to 600 (seconds) as the interval for retries to be performed if a log file cannot be read, or connection to the monitored host cannot be established. If this value is omitted, `3` (seconds) is assumed. The retry interval is the interval between the occurrence of an error and the next retry attempt.

`hold-count`

Specify a value from `1` to `100` as the number of JP1 events that can be held during retry processing. If this parameter is omitted, `100` is assumed. Executing a retry requires resources for holding JP1 events converted during retry processing. The amount of memory necessary for retry processing is as follows:

- *number-of-held-JP1-events* × 1 KB

`keep-event={ OLD | NEW }`

When the number of JP1 events held during retry processing exceeds the limit, the excess JP1 events are removed. Use either of the values below to specify the type of events (old JP1 events or new JP1 events) to be kept when the number of held JP1 events exceeds the limit. If this parameter is omitted, `OLD` is assumed.

`OLD`

Specify this value if you want to keep old JP1 events. If this value is specified, values not exceeding the number of JP1 events specified in `hold-count` are held, and any JP1 events generated thereafter are removed.

`NEW`

Specify this value if you want to keep new JP1 events. If this value is specified and the set number of held JP1 events is exceeded, the JP1 events are removed starting from the oldest events.

`unset-extattr`

Specify this value when you do not want to output an attribute. You can set this value when the version of JP1/Base is 10-50 or later. If you do not want to output the monitoring name, specify `TRAP_NAME`. If you do not want to output the monitoring ID, specify `TRAP_ID`. If you do not want to output either of them, specify `TRAP_NAME` and `TRAP_ID` by separating them with a comma (`,`). The following is a specification example of when the monitoring name and monitoring ID are not output:

Example:

```
TRAP_NAME,TRAP_ID
```

This parameter must be written in a line.

`FILETYPE={ SEQ | SEQ2 | WRAP2 }`

Specify the data output format of the log file to trap. If this parameter is omitted, `SEQ` is assumed.

For details about the data output format of the log file to trap, see *8.6.3(1) Output formats of log file trap information* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`HEADLINE`

Specify a value from 0 to 99,999 as the number of header lines when there is a header at the beginning of the log file to be read. If this parameter is omitted, it is assumed that there is no header.

Note that if the size of a character string in the specified header exceeds the upper limit for header size (10 kilobytes), an error occurs.

`MARKSTR=[!]"`*regular-expression*`"`

Specifies, using regular expressions, data that you do not want to monitor, such as data that is not log data. If this parameter is omitted, it is assumed that no data is excluded as data to be monitored. Enclose a regular expression in double-quotation marks (`"`). Data that is not log data refers to data that is output to a log file at a certain interval. The following are examples.

Example:

```
"==== 13:00:00 JP1/Base Event ===="
```

If an exclamation mark (`!`) is inserted before a double-quotation mark (`"`), the regular expression becomes an exclusion-condition and any data not matching the specified regular expression is not monitored.

You can specify multiple regular expressions for a single `MARKSTR` parameter. If multiple regular expressions are specified, the AND condition is applied. Therefore, the only data that is not subject to monitoring is the data that matches all the regular expression conditions, including the specification of the exclamation mark (`!`). Separate multiple regular expressions by a linefeed. On line 2 and subsequent lines, specify only values, and type at least one space before a value on each of the lines. The following example shows how to specify data that contains ==== and `MARK` as data that is not to be monitored:

Example:

```
MARKSTR="====" (linefeed)
ΔΔΔΔΔ"MARK"
```

Legend: Δ indicates a single-byte space.

This parameter can be specified multiple times. You can specify this parameter as many times as you wish. When multiple parameters are specified, the OR condition is applied, and any data that matches any specification is not monitored.

A regular expression specified for this parameter is checked from the beginning of the entered log data to the length specified by the `-m` option of the `jevlogstart` command. If this parameter is omitted, it is assumed that all data is log data.

`ACTDEF=[{EXIT}][`*event-level*`][`*event-ID*`][!]"`*regular-expression*`"`

Specifies a regular expression for the log data to be converted to JP1 events, event IDs corresponding to those JP1 events, and event levels. If this parameter is omitted, it is assumed that none of the above values are specified. If there is log data that matches the regular expression, a JP1 event is issued with the specified event ID. Do not use a space or a tab before or after =, `EXIT`, *event-level*, or *event-ID*. If you do so, a syntax error occurs.

`EXIT`

If multiple `ACTDEF` parameters are specified and log data matches a condition specified for `EXIT`, monitoring of the log data ends.

If multiple `ACTDEF` parameters are specified and one log data item matches multiple `ACTDEF` parameter conditions, JP1 events equal to the number of matched conditions are issued. If `EXIT` is specified, a JP1 event is issued with the event ID of the condition specified for `EXIT`, after which no more log data is monitored.

event-level

Specify the event level for the extended attribute of a JP1 event by enclosing it in left and right angle brackets (< and >). You can specify the following values:

`Emergency`

`Alert`

`Critical`

`Error`

`Warning`

`Notice`

`Information`

`Debug`

If this parameter is omitted, `Notice` is assumed.

event-ID

Specify an event ID for registering a JP1 event on an event server. Separate the first four bytes (basic code) and the last four bytes (extended code) of the event ID by a colon (`:`), and write the ID in hexadecimal notation. Use uppercase `A` to `F`. Note that the last four bytes (the four bytes after the colon) can be omitted, in which case `0` is assumed for the omitted value. Zeros (`0`) are also inserted for any non-specified digits, beginning on the left side, if either the first or last four bytes have fewer than eight digits. Use a user-specifiable value from `0:0` to `1FFF:0` and `7FFF8000:0` to `7FFFFFFF:0`. For an extended code, specify `0`. Event ID format examples are provided below.

Example:

The following three specifications have the same meaning:

```
0000011A:00000000
11A:0
11A
```

"*regular-expression*"

Specify the log data to be converted to a JP1 event in a regular expression. The regular expression you can use is fixed to the extended normal expression. Enclose a regular expression in double-quotation marks ("). If an exclamation mark (`!`) is inserted before the first double-quotation mark ("), the regular expression becomes an exclusion-condition and any data that does not match the specified regular expression is converted.

You can specify multiple regular expressions for a single `ACTDEF` parameter. If multiple regular expressions are specified, the AND condition is applied. Therefore, only data that matches all the regular expression conditions, including specification of the exclamation mark (`!`), is converted to JP1 events. Separate multiple regular expressions by a linefeed. On line 2 and subsequent lines, specify only values, and type at least one space before a value on each of the lines. The following example shows how to specify data that contains `jp1base` and `error` as data to be converted to the JP1 event with event ID `00000333`:

Example:

```
ACTDEF=00000333 "jp1base" (linefeed)
Δ Δ Δ Δ Δ"error"
```

Legend: Δ indicates a single-byte space.

More than one of this parameter can be specified. You can specify this parameter as many times as you wish. When multiple parameters are specified, the OR condition is applied, and any data that matches a specification is converted to JP1 events.

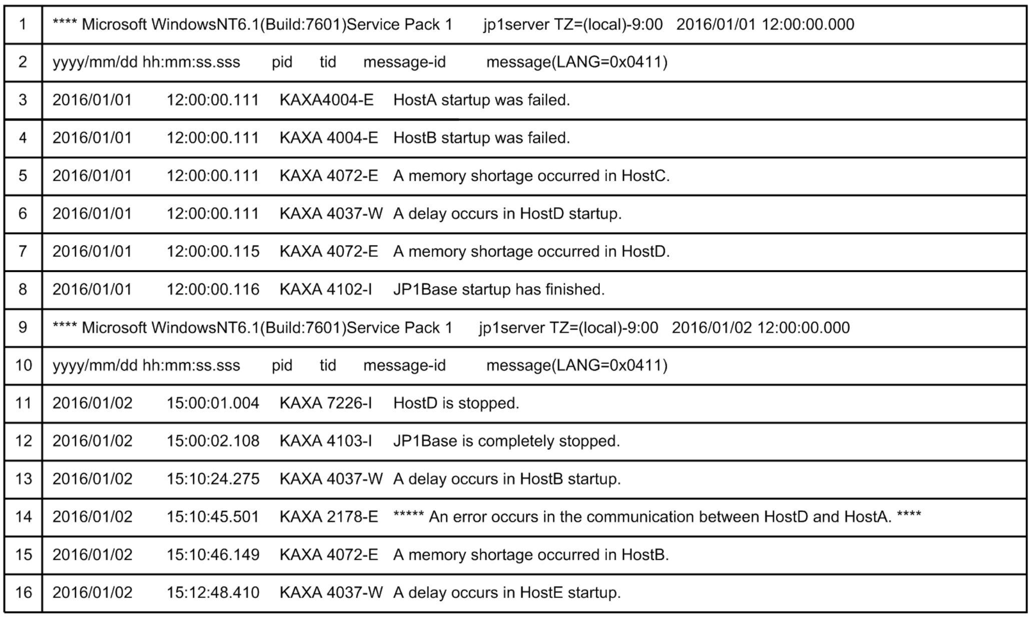
A regular expression specified for this parameter is checked from the beginning of the entered log data to the length specified as the *maximum length of data converted to an event for a startup option (bytes)*.

This parameter cannot be omitted.

Example definition

Example definition for the MARKSTR and ACTDEF parameters

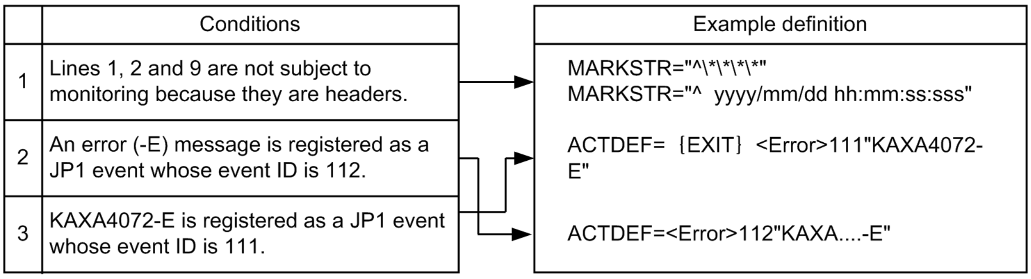
The following examples show example definitions for the MARKSTR and ACTDEF parameters based on the following log data.



1	**** Microsoft WindowsNT6.1(Build:7601)Service Pack 1 jp1server TZ=(local)-9:00 2016/01/01 12:00:00.000
2	yyyy/mm/dd hh:mm:ss.sss pid tid message-id message(LANG=0x0411)
3	2016/01/01 12:00:00.111 KAXA4004-E HostA startup was failed.
4	2016/01/01 12:00:00.111 KAXA 4004-E HostB startup was failed.
5	2016/01/01 12:00:00.111 KAXA 4072-E A memory shortage occurred in HostC.
6	2016/01/01 12:00:00.111 KAXA 4037-W A delay occurs in HostD startup.
7	2016/01/01 12:00:00.115 KAXA 4072-E A memory shortage occurred in HostD.
8	2016/01/01 12:00:00.116 KAXA 4102-I JP1Base startup has finished.
9	**** Microsoft WindowsNT6.1(Build:7601)Service Pack 1 jp1server TZ=(local)-9:00 2016/01/02 12:00:00.000
10	yyyy/mm/dd hh:mm:ss.sss pid tid message-id message(LANG=0x0411)
11	2016/01/02 15:00:01.004 KAXA 7226-I HostD is stopped.
12	2016/01/02 15:00:02.108 KAXA 4103-I JP1Base is completely stopped.
13	2016/01/02 15:10:24.275 KAXA 4037-W A delay occurs in HostB startup.
14	2016/01/02 15:10:45.501 KAXA 2178-E ***** An error occurs in the communication between HostD and HostA. ****
15	2016/01/02 15:10:46.149 KAXA 4072-E A memory shortage occurred in HostB.
16	2016/01/02 15:12:48.410 KAXA 4037-W A delay occurs in HostE startup.

Example definition 1

The log file trap conditions are listed on the left, and the example definition for the log file-trap action definition file is shown on the right.



	Conditions
1	Lines 1, 2 and 9 are not subject to monitoring because they are headers.
2	An error (-E) message is registered as a JP1 event whose event ID is 112.
3	KAXA4072-E is registered as a JP1 event whose event ID is 111.

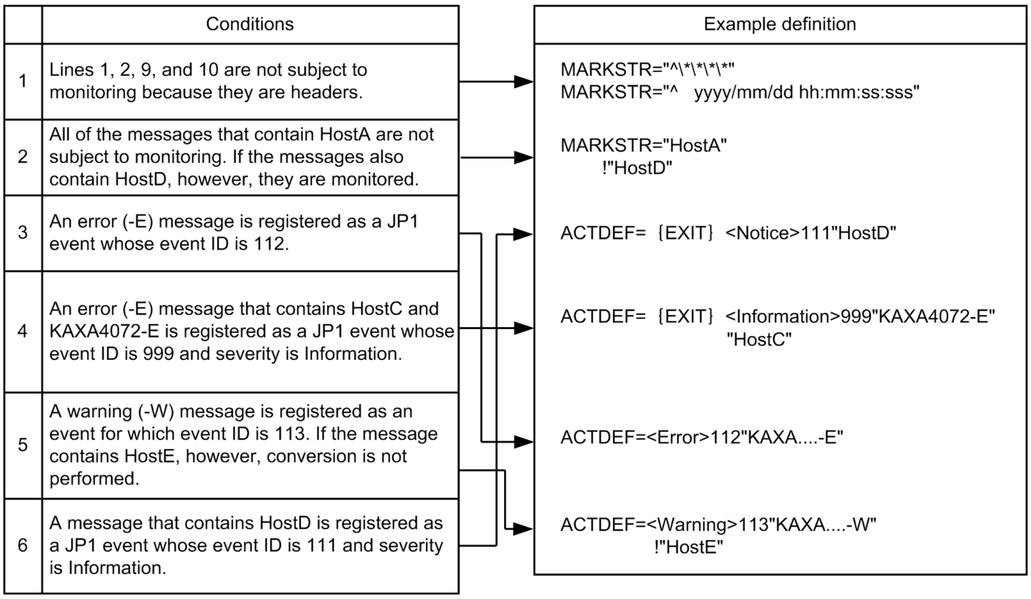
Example definition

```
MARKSTR="^\*\*\*\*"
MARKSTR="^  yyyy/mm/dd hh:mm:ss:sss"

ACTDEF= ｛EXIT｝ <Error>111"KAXA4072-
E"

ACTDEF=<Error>112"KAXA....-E"
```

●Matching conditions are applied in the defined order. When a definition is defined so that matching is performed in the order of condition 2 and condition 3, a message that contains KAXA4072-E matches condition 2 and condition 3. As a result, two JP1 events whose event IDs are 111 and 112 are registered. Because of this, define the matching order of condition 3 and condition 2, and then define {EXIT} so that the subsequent monitoring is not performed if condition 3 is matched.

Example definition 2

Log file trap conditions that are different from the conditions listed for example definition 1 are listed on the left, and the example definition for the log file-trap action definition file is shown on the right.



	Conditions
1	Lines 1, 2, 9, and 10 are not subject to monitoring because they are headers.
2	All of the messages that contain HostA are not subject to monitoring. If the messages also contain HostD, however, they are monitored.
3	An error (-E) message is registered as a JP1 event whose event ID is 112.
4	An error (-E) message that contains HostC and KAXA4072-E is registered as a JP1 event whose event ID is 999 and severity is Information.
5	A warning (-W) message is registered as an event for which event ID is 113. If the message contains HostE, however, conversion is not performed.
6	A message that contains HostD is registered as a JP1 event whose event ID is 111 and severity is Information.

Example definition

```
MARKSTR="^\*\*\*\*"
MARKSTR="^   yyyy/mm/dd hh:mm:ss:sss"

MARKSTR="HostA"
       !"HostD"

ACTDEF= {EXIT} <Notice>111"HostD"

ACTDEF= {EXIT} <Information>999"KAXA4072-E"
                             "HostC"

ACTDEF=<Error>112"KAXA....-E"

ACTDEF=<Warning>113"KAXA....-W"
              !"HostE"
```

●Matching conditions are applied in the defined order. When a definition is defined so that matching is performed in the order of condition 3 and condition 4, two JP1 events whose event IDs are 112 and 999 are registered for a message that contains KAXA4072-E and HostC. Because of this, define the matching order of condition 4 and condition 3, and then define {EXIT} so that the subsequent monitoring is not performed if condition 4 is matched.

●If {EXIT} is not defined for condition 6, JP1 events whose IDs are 111 and 112 are registered for error messages that contain HostD, and JP1 events whose event IDs are 111 and 113 are registered for warning messages that contain HostD.

Remote-monitoring event log trap action-definition file

Format

```
retry-times number-of-retries
retry-interval retry-interval
open-retry-times number-of-retries-for-event-log-collection
open-retry-interval retry-interval-for-event-log-collection
trap-interval monitoring-interval
matching-level comparison-level
filter-check-level filter-check-level
# filter
filter log-type [id=event-ID] [trap-name=log-file-trap-name]
    conditional-statement-1
    conditional-statement-2
      :
    conditional-statement-n
end-filter
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines the actions of the event log trapping function for remote monitoring. Its contents of the file are referenced when the remote monitoring event log trapping function is started.

If you use UTF-8 as the encoding to save a file, save the file without attaching a BOM (byte order mark).

When the definitions are applied

The settings for the remote-monitoring event log trap action-definition file take effect at the following times:

- When a reload or restart operation is executed from the Display/Edit Profiles window

  For details about the Display/Edit Profiles window, see *5.9 Display/Edit Profiles window* in the *JP1/Integrated Management 3 - Manager GUI Reference*.

- When the `jcfaleltstart` or `jcfaleltreload` command is executed

  For details about the `jcfaleltstart` command, see *jcfaleltstart (Windows only)*in *Chapter 1. Commands*. For details about the `jcfaleltreload` command, see *jcfaleltreload (Windows only)* in *Chapter 1. Commands*.

- When JP1/IM - Manager is restarted

Information that is specified

`retry-times`

Specify a value from 0 to 86,400 for the number of retries to be attempted when a connection to an event service cannot be established due to a temporary communication failure. If this parameter is omitted, no retry operation is performed. If the specified number of retries has been attempted but none have been successful, an error occurs. By combining `retry-times` and `retry-interval`, you can set a time equal to or longer than 24 hours, but if you do so and 24 hours or more passes after a retry attempt starts, retry processing stops.

`retry-interval`

Specify a value from 1 to 600 (seconds) for the interval between retries to be performed when a connection to an event service could not be established due to a temporary communication failure. If this value is omitted, 10 seconds is assumed.

`open-retry-times`

Specify a value from 1 to 3,600 as the number of times to retry the event log collection processing when the processing fails or the connection to the monitored host fails. If this value is omitted, a retry count of 3 times is assumed. When the specified number of retries is exceeded, the monitoring of log files stops.

`open-retry-interval`

Specify a value from 3 to 600 (seconds) as the interval between retries when the event log collection processing fails or the connection to the monitored host fails. If this value is omitted but a value is specified for `trap-interval`, the value specified for `trap-interval` is assumed. If `trap-interval` is not specified, 300 seconds is assumed. The retry interval is the length of time before a retry is attempted after an error occurs.

`trap-interval`

Specify a value from 60 to 86,400 (seconds) as the interval for monitoring event logs. If this value is omitted, 300 (seconds) is assumed. Event log traps monitor event logs at a fixed interval.

`matching-level`

Specify the comparison level of an event log and the definition if the explanatory text of an event log cannot be read because the message DLL or the category DLL is not set correctly when the `message` or `category` attribute is specified for a filter. If `0` is specified, the items are not compared, but are compared with the next filter. If `1` is specified, the items are compared. If this parameter is omitted, `0` is assumed.

`filter-check-level`

Specify the check level when an invalid log type (a type non-existent in the system) or an invalid regular expression is specified for a filter. If `0` is specified and a filter contains an invalid log type or regular expression, the applicable filter is disabled. If at least one valid filter exists, the remote-monitoring event log trap is started or loaded successfully. If there is no valid filter, the remote-monitoring event log trap fails to start or reload. If `1` is specified and the filter has at least one invalid log type or regular expression, the remote-monitoring event log trap fails to start or reload.

If this parameter is omitted, `0` is assumed.

`filter` to `end-filter`

log-type

Specify the type of event log to be monitored.

Example:

```
Application
Security
System
DNS Server
Directory Service
File Replication Service
```

`DFS Replication`

When the same log type is specified for multiple filters, the condition is satisfied if the conditions for any one of the filters are met.

`[id=`*event-ID*`]`

Specify an event ID for registering a JP1 event on an event server. Write the ID in hexadecimal notation and separate the first four bytes (basic code) and the last four bytes (extended code) of the event ID by a colon (`:`). When entering hexadecimal notation, use uppercase `A` to `F`. Note that the last four bytes (the four bytes after the colon) can be omitted, in which case `0` is assumed for the omitted value. Zeros (`0`) are also inserted for any non-specified digits, beginning on the left side, if either the first or last four bytes have fewer than eight digits. Use a user-specifiable value from `0:0` to `1FFF:0` and `7FFF8000:0` to `7FFFFFFF:0`. There can be no space or tab between `id=` and the value. However, there must be a space between *log-type* and *log-file-trap-name*. If you omit this value, event ID `00003A71` is assumed. Event ID format examples are provided below.

Example:

The following three specifications have the same meaning:

```
0000011A:00000000
11A:0
11A
```

`[trap-name=`*log-file-trap-name*`]`

Specify a log file trap name to determine the corresponding filter for the registered JP1 event converted from the event log. The first character of *log-file-trap-name* must be an alphanumeric character. Uppercase and lowercase are distinguished. Do not add a space or tab. If this parameter is omitted, the extended attribute `E.JP1_TRAP_NAME` is not created at the time of JP1 event conversion.

`conditional-statement`

The following explains the *conditional-statement*:

When a value other than `type` is specified for the attribute:

attribute-specification regular-expression-1 regular-expression-2 regular-expression-3...

When `type` is specified for the attribute

`type` *log-type-1 log-type-2 log-type-3...*

The above condition is satisfied if any of regular expressions (or log type) listed after the attribute specification exists. Note that the AND condition is applied to the conditional statements in the filter, and the OR condition is applied between filters.

Attribute settings

The following table explains the attribute settings.

Attribute name	Description
`type`	Log type
`source`	Source
`category`	Category
`id`	Event ID
`user`	User
`message`	Description
`computer`	Computer name

Note

When `message` is set as the attribute, an event log that contains `Description related to xxx was not found` (wording used when a message DLL is not found) as part of its description will not be able to generate a message. As a result, the log is excluded as a trap target. If character strings to be trapped are contained in the inserted paragraph, the log is not trapped.

In the above case, make sure that the message DLL mentioned in the event log description is properly configured in accordance with the Windows event log mechanism. If the message DLL is not properly configured, the log might fail to be trapped because the description cannot be read from the event log. If you want to trap a message with no message DLL, set the `matching-level` parameter to 1.

For details about the log information that can be monitored, see *8.6.3 Log information that can be monitored* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Regular expressions

A regular expression is expressed as a character string enclosed in single quotation marks (`'`) and is specified as `'`*xxxxx*`'`. In the form `!'...'`, with an exclamation mark preceding the initial single quotation mark, the character string is any string other than the specified character string. If you want to specify a single quotation mark (`'`) as part of a regular expression, enter an escape sequence such as `\'`. Regular expressions can be specified only when the log type is not `type`.

Log types

The following table lists and describes the log types.

Log type	Description	Event level
Information	Information	Information
Warning	Warning	Warning
Error	Error	Error
Audit_success	Successful audit	Notice
Audit_failure	Failed audit	Notice

Example definition

Example definition 1: OR and AND conditions

Example definition for the OR condition

When the log type is *system log*, and `TEXT`, `MSG`, or `-W` is contained in the description.

```
filter "System"
    message 'TEXT' 'MSG' '-W'
end-filter
```

If you separate conditions with a space or a tab, the OR condition is applied.

Example definition for the AND condition

When the log type is *system log*, and `TEXT`, `MSG`, and `-W` are all contained in the description.

```
filter "System"
    message 'TEXT'
    message 'MSG'
    message '-W'
end-filter
```

If you separate conditions with a linefeed, the AND condition is applied. After a linefeed, start a new line with the attribute name.

Example definition 2: Setting multiple filters

Trap event logs whose log type is *application log* and that satisfy the following condition:

filter-1

Type: Application log

Category: Error

Description: Contains `-E` and `JP1/Base`.

filter-2

Type: Application log

Category: Warning

Description: Contains `-W` or `warning`.

```
#filter-1
filter "Application"
    type Error
    message '-E'
    message 'JP1/Base'
end-filter
#filter-2
filter "Application"
    type Warning
    message '-W' 'warning'
end-filter
```

Example definition 3: Using regular expressions

Traps event logs that satisfy the following conditions:

- Type: Application log
- Category: Error
- Event ID: `111`
- Description: Contains `-E` or `MSG`, but not `TEXT`.

```
filter "Application"
    type Error
    id '^111$'
    message '-E' 'MSG'
    message !'TEXT'
end-filter
```

If you want to set event ID `111` as a condition, specify the regular expression `id '^111$'`. Specifying `id '111'` creates a condition that means that *the value 111 is included in the ID*. Therefore, an event ID such as `1112` or `0111` satisfies the condition. If an exclamation mark (`!`) is inserted before the first single quotation mark, any data that does not match the specified regular expression is selected. The regular expression is fixed to the extended regular expression of JP1/Base. For details about extended regular expressions, see the description about the regular expression syntax in the *JP1/Base User's Guide*.

Example definition 4: Do not convert specific event logs

Do not trap event logs whose log type is *system log*, whose event level is warning, and which satisfy the following conditions:

- Source: AAA
- Event ID: `111`
- Description: Contains `TEXT`.

```
#Event logs for which source is AAA are not trapped.
```

```
filter "System"
    type Warning
    source !'AAA'
end-filter
#Event logs for which source is AAA, and event ID is a value other than 111 are trapped.
filter "System"
    type Warning
    source 'AAA'
    id !'^111$'
end-filter
#Event logs for which source is AAA and event ID is 111, but whose description does not include TEXT are trapped.
filter "System"
    type Warning
    source 'AAA'
    id '^111$'
    message !'TEXT'
end-filter
```

Setup information file (jimdbsetupinfo.conf)

Format

```
#IM DATABASE SERVICE - DB Size
IMDBSIZE=value
#IM DATABASE SERVICE - Data Storage Directory
IMDBDIR=value
#IM DATABASE SERVICE - Port Number
IMDBPORT=value
#IM DATABASE SERVICE - DB Install Directory
IMDBENVDIR=value
#IM DATABASE SERVICE - Host Name
IMDBHOSTNAME=value
```

File

`jimdbsetupinfo.conf` (setup information file)

`jimdbsetupinfo.conf.model` (model file for the setup information file)

Storage directory

In Windows

Manager-path`\conf\imdb\setup\`

In UNIX

`/etc/opt/jp1imm/conf/imdb/setup/`

Description

This file specifies setup information, such as the size of the IM database and the directory for storing data for the IM database, when the integrated monitoring database and IM Configuration Management database are set up.

The setup information file is shared during setup of the integrated monitoring database and IM Configuration Management database. If you have set up one of the databases (integrated monitoring database or IM Configuration Management database) first and then are creating the other one, you must specify for the second database the same values as were specified for the first database.

The table below describes the approximate amount of disk space used per size of the IM database, which you must specify in the setup information file.

Note that, in addition to the areas described in the table below, approximately 0.2 gigabytes of free space is required in the directory in which to install the IM database (`IMDBENVDIR`), whatever the size of the IM database. For details about the specific amount of disk space used, see the Release Notes for JP1/IM - Manager. We recommend that you use the values provided in the Release Notes for JP1/IM - Manager when you estimate the amount of disk space used.

Table 2–87: Sizes of databases that are created

Size	System database area#1, #2 (gigabytes)	Integrated monitoring database area#1, #3 (gigabytes)	IM Configuration Management database area#1, #4 (gigabytes)	Total (gigabytes)
S	2	9	2	13

Size	System database area#1, #2 (gigabytes)	Integrated monitoring database area#1, #3 (gigabytes)	IM Configuration Management database area#1, #4 (gigabytes)	Total (gigabytes)
M	3	33	2	38
L	7	98	11	116

#1

The system database area, the integrated monitoring database area, and the IM Configuration Management database area are created immediately under the database storage directory (`IMDBDIR`) specified in the setup information file.

#2

Area shared by the IM Configuration Management database and integrated monitoring database created during setup of the IM database.

#3

Area created when the `jcodbsetup` command is executed.

#4

Area created when the `jcfdbsetup` command is executed.

When the definitions are applied

The contents of this file are loaded during setup and the IM database environment is configured based on the value specified for each item.

Information that is specified

`IMDBSIZE`

Specifies the size of the IM database to be created as the uppercase letter `S`, `M`, or `L`. The default is `S`.

`IMDBDIR`

Specifies the absolute path of the directory in which data for the IM database is to be stored. JP1/IM creates the `imdb` directory immediately under the specified directory and then stores the IM database file (area). The default is as follows:

- In Windows: *Manager-path*`\database`

  An error results if a network drive or Windows reserved device file is specified. If the specified directory cannot be found, command execution fails. You must create the directory before executing the command.

- In UNIX: `/var/opt/jp1imm/database`

  Specify a directory whose status is *mounted*. Do not specify a directory that is easily unmounted. If the directory is unmounted during operation, database startup and access will fail. If the specified directory cannot be found, command execution fails. You must create the directory before executing the command.

  For details about the necessary directory permissions, see *Table 2-88 Correspondence between OS and directory permissions*.

The following explains the character string that can be used in the absolute path format:

- In Windows:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, \, `(`, `)`, and `.` (period). This character string must begin with the drive name.

- In UNIX:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, `/`, and `.` (period). This character string must begin with the path delimiter (`/`).

`IMDBPORT`

Specifies the port number used by the IM database. The permitted value range is from `5001` to `65535`. The default is `20700`.

This port number must be different from any of the following port numbers:

- Port numbers specified when other logical hosts were set up
- Port numbers specified in the `services` file#
- Port numbers used in other products' HiRDB installation
- Temporary port numbers used by other products and the OS

#: Make sure that you do not specify the port number set in `IMDBPORT` in the `services` file.

`IMDBENVDIR`

Specifies the absolute path of the directory in which the IM database is to be installed. Creates a directory under the specified directory (`JM`*n*: *n* matches `LOGICALHOSTNUMBER`), and then install the IM database.

- In Windows: *Manager-path*`\dbms`

  An error results if a network drive or Windows reserved device file is specified. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

- In UNIX: `/var/opt/jp1imm/dbms`

  Specify a directory that is in mounted status. Do not specify a directory that is easily unmounted. If the directory is unmounted during operation, database startup and access will fail. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command. In addition, do not specify a path that contains a symbolic link.

  The following table explains the directory permissions.

Table 2–88: Correspondence between OS and directory permissions

OS	Permission
Linux	Owner: root Group: root Mode: 755

The following explains the character string that can be used in the absolute path format:

- In Windows:

  A string of no more than 195 characters, consisting of alphanumeric characters, `_`, `\`, `(`, `)`, and the space. This character string must begin with the drive name.

- In UNIX:

  A string of no more than 123 characters, consisting of alphanumeric characters, `_`, `/`, and `.` (period). This character string must begin with the path delimiter (`/`).

`IMDBHOSTNAME`

Specifies the host name or the IP address to be used for communication with JP1/IM - MO and JP1/OA running on another host. If there is no linkage with JP1/IM - MO and JP1/OA on other hosts, do not define the line that specifies this item.

By default, a local host name is specified. If this value is omitted, the local host name is assumed. You can specify a maximum of 32 characters. Specifiable characters are alphanumeric characters, the hyphen (`-`), the underscore (`_`), the at mark (`@`), and the period (`.`).

Example definition

```
#IM DATABASE SERVICE - DB Size
IMDBSIZE=S
#IM DATABASE SERVICE - Data Storage Directory
IMDBDIR=Manager-path\database
#IM DATABASE SERVICE - Port Number
IMDBPORT=20700
#IM DATABASE SERVICE - DB Install Directory
IMDBENVDIR=Manager-path\dbms
#IM DATABASE SERVICE - DB Host Name
IMDBHOSTNAME=
```

Cluster setup information file (jimdbclustersetupinfo.conf)

Format

```
#IM DATABASE SERVICE - Logical Host Number
LOGICALHOSTNUMBER=value
#IM DATABASE SERVICE - Logical Host Name
LOGICALHOSTNAME=value
#IM DATABASE SERVICE - DB Size
IMDBSIZE=S
#IM DATABASE SERVICE - Port Number
IMDBPORT=value
#IM DATABASE SERVICE - Data Storage Directory (Local Work Area)
IMDBDIR=Manager-path\db
#IM DATABASE SERVICE - Data Storage Directory (Shared Data Area)
SHAREDBDIR=shared-directory\db
#IM DATABASE SERVICE - Online Host Name
ONLINEHOSTNAME=value
#IM DATABASE SERVICE - DB Install Directory
IMDBENVDIR=Manager-path\dbms
```

File

`jimdbclustersetupinfo.conf` (cluster setup information file)

`jimdbclustersetupinfo.conf.model` (model file for the cluster setup information file)

Storage directory

In Windows

Manager-path`\conf\imdb\setup\`

In UNIX

`/etc/opt/jp1imm/conf/imdb/setup/`

Description

This file specifies the IM database size for a logical host, or the directory for storing data of the IM database for a logical host when the integrated monitoring database and IM Configuration Management database are set up in a cluster environment.

The cluster setup information file is shared during setup of the integrated monitoring database and IM Configuration Management database. If you have set up one of the databases (integrated monitoring database or IM Configuration Management database) first and then are creating the other one, you must specify for the second database the same values as were specified for the first database. If you are configuring a cluster environment, when you set up the secondary node, copy the cluster setup information file used for the primary node. If you set up multiple logical hosts on the same host, you must copy `jimdbclustersetupinfo.conf` (cluster setup information file) under a different name and change the settings.

The table below describes the approximate amount of disk space used per size of the IM database, which you must specify in the cluster setup information file.

Note that, in addition to the areas described in the table below, approximately 0.2 gigabytes of free space is required in the directory in which to install the IM database (`IMDBENVDIR`), whatever the size of the IM database. For details about the specific amount of disk space used, see the Release Notes for JP1/IM - Manager. We recommend that you use the values provided in the Release Notes for JP1/IM - Manager when you estimate the amount of disk space used.

Table 2–89: Sizes of databases that are created

Size	Local disk	Shared disk			
	System database area (local disk)#1 (gigabytes)	System database area (shared disk)#2 (gigabytes)	Integrated monitoring database area#2 (gigabytes)	IM Configuration Management database area#2 (gigabytes)	Total (gigabytes)
S	0.1	2	9	2	13
M	0.1	3	33	2	38
L	0.2	7	98	11	116

#1

The system database area (local disk) is created immediately under the local database storage directory (`IMDBDIR`) specified in the cluster setup information file.

#2

The system database area (shared disk), the integrated monitoring database area, and the IM Configuration Management database area are created immediately under the shared database storage directory (`SHAREDBDIR`) specified in the cluster setup information file.

When the definitions are applied

The contents of this file are loaded during setup, and the IM database environment for a logical host is configured based on the value specified for each item.

Information that is specified

`LOGICALHOSTNUMBER`

Specify a value from 1 to 9 as the number to identify a logical host in the IM database for a logical host.

If you add a logical host, you must specify a different number. Specify the same number for both primary and secondary nodes.

`LOGICALHOSTNAME`

Specify the name of a logical host. This must be a logical host name that can be resolved, and specified in the `jp1cohasetup` and `jp1cc_setup_cluster` commands. The IM database does not reference the `jp1hosts` and `jp1hosts2` files. Therefore, for `LOGICALHOSTNAME`, specify a logical host name whose name is in the `hosts` file or can otherwise be resolved using the OS's name resolution capability. You can specify a string of up to 32 characters that consist of half-width alphanumeric characters and hyphens (`-`).

The logical host name is case sensitive. As the logical host name, specify the logical host name set in JP1/Base in the correct format, especially case. For details on how to set up JP1/Base on a logical host, see the sections below in the *JP1/Integrated Management 3 - Manager Configuration Guide*:

- In Windows
  See *7.4.3(2) Setting up JP1/Base*
- In UNIX

See *8.4.3(2) Setting up JP1/Base*

`IMDBSIZE`

Specify the size of the IM database for a logical host to be created by using uppercase letters `S`, `M`, or `L`. The default is `S`.

IMDBDIR

Specify the absolute path of the directory in which data of the IM database for a logical host is to be stored. Do not specify the shared disk in a cluster. JP1/IM creates the imdb directory immediately under the specified directory, and then stores the IM database file (for a local work area).

- In Windows:

  An error results if a network drive or Windows reserved device file is specified. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

- In UNIX:

  Specify a directory that is in mounted status. Do not specify a directory that is easily unmounted. If the directory is unmounted during operation, database startup and access will fail. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

  The following table describes the directory permissions.

Table 2–90: Correspondence between OS and directory permissions

OS	Permission
Linux	Owner: root Group: root Mode: 755

The following shows the character string that can be used in the absolute path format:

- In Windows:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, \, (,), and . (period). This character string must begin with the drive name.

- In UNIX:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, /, and . (period). This character string must begin with the path delimiter (/).

IMDBPORT

Specify the port number used by the IM database for a logical host. The permitted value range is from 5001 to 65535.

This port number must be different from any of the following port numbers:

- Port numbers specified when other logical hosts were set up
- Port numbers specified in the services file#
- Port numbers used in other products' HiRDB installation
- Temporary port numbers used by other products and the OS

#: Make sure that you do not specify the port number set in IMDBPORT in the services file.

SHAREDBDIR

Specifies the absolute path of the directory in which data of the IM database for a logical host that is shared by the primary and secondary nodes in a cluster configuration is to be stored. Specify a directory on a shared disk. JP1/IM creates the imdb directory immediately under the specified directory, and stores the IM database files (for the shared data area) for a logical host.

The following shows the character string that can be used in the absolute path format:

- In Windows:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, \, (,), and . (period). This character string must begin with the drive name.

An error results if a network drive or Windows reserved device file is specified. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

- In UNIX:

  A string of no more than 95 characters, consisting of alphanumeric characters, _, /, and . (period). This character string must begin with the path delimiter (/).

  Specify a directory that is in mounted status. Do not specify a directory that is easily unmounted. If the directory is unmounted during operation, database startup and access will fail. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command. For details about the necessary directory permissions, see *Table 2-90Correspondence between OS and directory permissions*.

ONLINEHOSTNAME

Specifies the host name of the primary node. Specify a host name that can be resolved for the primary node. You can specify a string of up to 32 characters that consist of half-width alphanumeric characters, hyphens (-), and periods (.). The executing host name is also case sensitive. Specify the executing host name in the correct form, especially case.

IMDBENVDIR

Specify the absolute path of the directory in which the IM database for a logical host is to be installed. Do not specify a shared disk in the cluster. Create a directory (JM*n*: *n* matches LOGICALHOSTNUMBER) immediately under the specified directory, and then install the IM database for a logical host. The default is as follows:

- In Windows: *Manager-path*\dbms

  An error results if a network drive or Windows reserved device file is specified. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

- In UNIX: /var/opt/jp1imm/dbms

  Specify a directory that is in mounted status. Do not specify a directory that is easily unmounted. If the directory is unmounted during operation, database startup and access will fail. If the specified directory does not exist, command execution fails. Make sure that you create the directory before you execute the command.

  For details about the necessary directory permissions, see *Table 2-90 Correspondence between OS and directory permissions*.

The following shows the character string that can be used in the absolute path format: In addition, do not specify a path that contains a symbolic link.

- In Windows:

  A string of no more than 195 characters, consisting of alphanumeric characters, _, \, (,), and the space. This character string must begin with the drive name.

- In UNIX:

  A string of no more than 123 characters, consisting of alphanumeric characters, _, /, and . (period). This character string must begin with the path delimiter (/).

Example definition

```
#IM DATABASE SERVICE - Logical Host Number
LOGICALHOSTNUMBER=1
#IM DATABASE SERVICE - Logical Host Name
LOGICALHOSTNAME=host1
#IM DATABASE SERVICE - DB Size
IMDBSIZE=S
#IM DATABASE SERVICE - Data Storage Directory (Local Work Area)
IMDBDIR=Manager-path\db
#IM DATABASE SERVICE - Port Number
```

```
IMDBPORT=20750
#IM DATABASE SERVICE - Data Storage Directory (Shared Data Area)
SHAREDBDIR=shared-directory\db
#IM DATABASE SERVICE - Online Host Name
ONLINEHOSTNAME=host_H1
#IM DATABASE SERVICE - DB Install Directory
IMDBENVDIR=Manager-path\dbms
```

Intelligent Integrated Management Database setup information file (jimgndbsetupinfo.conf)

Format

```
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=port-number-for-intelligent-integrated-management-database
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=trend-data-management-service-port-number
#IM GNDATABASE SERVICE - Data Storage Directory
IMGNDBDIR=data-storage-directory-for-intelligent-integrated-management-database
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=directory-where-intelligent-integrated-management-database-is-installed
#IM GNDATABASE SERVICE - Retention
RETENTION=retention-period-of-time-series-data-in-trend-data-management-DB
#IM GNDATABASE SERVICE - Username
USERNAME=user-name-of-OS-used-to-start-intelligent-integrated-management-database
# TREND DATA DATABASE - MAX DISK SIZE [GB]
TDDBDISKMAX=max-disk-requirements-of-trend-data-management-database
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=truncation-duration-when-trend-data-is-deleted
```

File

`jimgndbsetupinfo.conf`[#]

`jimgndbsetupinfo.conf.model` (model file)

#: The installer creates it from a duplicate of the model file by deleting extension "`.model`".

Storage directory

In Windows

Manager-path`\conf\imgndb\setup\`

In UNIX

`/etc/opt/jp1imm/conf/imgndb/setup/`

Description

A file that describes the definitions that are required during the setup of the Intelligent Integrated Management database.

Character code

ASCII (You cannot specify multi byte characters.)

When the definitions are applied

At setup time (when the jimgndbsetup command is executed), the contents of this file are read and the environment of the intelligent integrated management database is built with the values specified for each item.

Information that is specified

`IMGNDBPORT=`*port-number-for-intelligent-integrated-management-database*

Specifies port number used by the Intelligent Integrated Management database.

The port number specified must be unique for each host that Setup creates.

The default is 20705. If omitted, the default value is assumed.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. The extension of the command restarts the service and takes effect.

`TDMSPORT=`*trend-data-management-service-port-number*

Specifies the port number used by the Trend Data Management Service.

The port number that you specify must be unique for each system and host that Setup creates.

The default is 20706. If omitted, the default value is assumed.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. The extension of the command restarts the service and takes effect.

`IMGNDBDIR=`*data-storage-directory-for-intelligent-integrated-management-database*

Specifies the absolute path of the directory in which the data of the Intelligent Integrated Management database is stored.

- In Windows

  Specify a character string of up to 100 single-byte alphanumeric characters, including "_" (underscore), "\", "(", ")", and "." (period), and single-byte spaces.

- In Linux

  Specify a character string of up to 100 single-byte alphanumeric characters, including "_" (underscore), "/" (slash), and "." (period).

During setup, create an imgndb directory directly under the specified directory and build a trend data management DB. If the trend data management DB has already been built, it cannot be changed from the specified contents at the time of construction.

The defaults are following:

In Windows: *Manager-path*`\database`

In Linux: `/var/opt/jp1imm/database`

If omitted, the default value is assumed.

`IMGNDBENVDIR=`*directory-where-intelligent-integrated-management-database-is-installed*

Specifies the absolute path of the directory where the Intelligent Integrated Management Database to be installed.

- In Windows

  Specify a character string of up to 200 single-byte alphanumeric characters, including "_" (underscore), "\", "(", ")", and "." (period), and single-byte spaces.

- In Linux

  Specify a character string of up to 200 single-byte alphanumeric characters, including "_" (underscore), "/" (slash), and "." (period).

During setup, `imgndbbin` directory is created directly under the specified directory, and the Intelligent Integrated Management Database is expanded. If you have already built an Intelligent Integrated Management Database, you cannot change it from the specification at the time of construction.

The defaults are following:

In Windows: *Manager-path*`\dbms`

In Linux: `/var/opt/jp1imm/dbms`

If omitted, the default value is assumed.

`RETENTION=`*retention-period-of-time-series-data-in-trend-data-management-DB*

Specify the retention period (unit: days) of the data stored in the trend data management DB.

The range is 1 to 1096.

The default is 32. If omitted, the default value is assumed.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. The extension of the command restarts the service and takes effect.

`USERNAME=`*user-name-of-OS-used-to-start-intelligent-integrated-management-database*

Specifies OS username from which the Intelligent Integrated Management Database is to be started in Linux (users who actually exist and are available for Login by users other than root). If specified in Windows configuration, it is ignored.

There is no default value. This specification is not optional.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. The extension of the command restarts the service and takes effect.

`TDDBDISKMAX=`*max-disk-requirements-of-trend-data-management-database*

Specifies the upper limit (in gigabytes) of the disk space required for Trend data Management Database. Automatic Delete occurs when Trend data Management Database disk requirements exceed 90% of this Value. If 0 is specified, the upper limit is not Setup.

The range is 0 or 10 to 131,072.

The default is 150. If the specification is omitted, the default Value is assumed.

If you want to change Setup during operation, change this Value and Execute `jimgndbsetup` command. Restart the service with the extension of the command. It will be reflected.

Notes:

When using monitoring Trend data Management Database Disk Requirements feature, we recommend that you specify a Value that exceeds the 10-day data size of the trend data stored in Trend data Management Database.

`TDDBCUTOFFTERM=`*truncation-duration-when-trend-data-is-deleted*

Specifies the duration (in days) of the trend data to delete when trend data management database disk requirements reach 90% of the size specified for `TDDBDISKMAX`. If `TDDBDISKMAX` is 0, this field is ignored.

The range is 1 to 31.

The default is 7. If the specification is omitted, the default Value is assumed.

If you want to change setup during operation, change this value and Execute `jimgndbsetup` command. Restart the service with the extension of the command. It will be reflected.

Example definition

- In Windows

```
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=20705
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=20706
#IM GNDATABASE SERVICE - Data Storage Directory
IMGNDBDIR=C:\Program Files (x86)\Hitachi\JP1IMM\database
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=C:\Program Files (x86)\Hitachi\JP1IMM\dbms
# IM GNDATABASE SERVICE - Retention
RETENTION=32
# TREND DATA DATABASE - MAX DISK SIZE [GB]
```

```
TDDBDISKMAX=764
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=7
```

- In Linux

```
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=20705
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=20706
#IM GNDATABASE SERVICE - Data Storage Directory
IMGNDBDIR=/var/opt/jp1imm/database
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=/var/opt/jp1imm/dbms
# IM GNDATABASE SERVICE - Retention
RETENTION=32
# IM GNDATABASE SERVICE - Username
USERNAME=USER01
# TREND DATA DATABASE - MAX DISK SIZE [GB]
TDDBDISKMAX=764
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=7
```

Cluster environment Intelligent Integrated Management Database setup information file (jimgndbclustersetupinfo.conf)

Format

```
#IM DATABASE SERVICE - Logical Host Name
LOGICALHOSTNAME=logical-host-name-of-the-intelligent-integrated-management-database
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=port-number-for-intelligent-integrated-management-database
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=trend-data-management-service-port-number
#IM DATABASE SERVICE - Data Storage Directory (Shared Data Area)
SHAREGNDBDIR=data-storage-directory-for-intelligent-integrated-management-database
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=directory-where-intelligent-integrated-management-database-is-installed
#IM DATABASE SERVICE - Logical Host Number
LOGICALHOSTNUMBER=logical-host-number
#IM GNDATABASE SERVICE - Retention
RETENTION=retention-period-of-time-series-data-in-trend-data-management-DB
#IM GNDATABASE SERVICE - Username
USERNAME=user-name-of-OS-used-to-start-intelligent-integrated-management-database
# TREND DATA DATABASE - MAX DISK SIZE [GB]
TDDBDISKMAX=max-disk-requirements-of-trend-data-management-database
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=truncation-duration-when-trend-data-is-deleted
```

File

`jimgndbclustersetupinfo.conf`#

`jimgndbclustersetupinfo.conf.model` (model file)

#: The installer creates it from a duplicate of the model file by deleting extension "`.model`".

Storage directory

In Windows

  Manager-path`\conf\imgndb\setup\`

In UNIX

  `/etc/opt/jp1imm/conf/imgndb/setup/`

Description

This file describes the definitions required when setting up a clustered environment for the Intelligent Integrated Management database.

Character code

ASCII (You cannot specify multi byte characters.)

When the definitions are applied

When setting up a clustered environment (when execution of `jimgndbsetup` command (with `-h` option specified)), this file is read and value specified for the items builds Intelligent Integrated Management Database environment for logical host.

Information that is specified

`LOGICALHOSTNAME=`*logical-host-name-of-the-intelligent-integrated-management-database*

Specifies the logical host name of the Intelligent Integrated Management database.

You can specify a character string of up to 63 bytes consisting of single-byte alphanumeric characters and hyphens (-). Uppercase and lowercase letters are sensitive.

If the value is empty or omitted, the value specified on the -h option of the jimgndbsetup command is used when the jimgndbsetup command is run.

Also, the logical host name must be a host name that can be resolved on the OS.

There is no default value.

`IMGNDBPORT=`*port-number-for-intelligent-integrated-management-database*

Specifies port number used by Intelligent Integrated Management Database.

The port number specified must be unique for each host that Setup creates.

There is no default value. This specification is not optional.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. In a logical host environment, the service remains stopped rather than restarted due to command extensions, so you must manually start the service after running the command.

`TDMSPORT=`*trend-data-management-service-port-number*

Specifies the port number used by the Trend Data Management Service.

The port number that you specify must be unique for each system and host that Setup creates.

There is no default value. This specification is not optional.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. In a logical host environment, the service remains stopped rather than restarted due to command extensions, so you must manually start the service after running the command.

`SHAREGNDBDIR=`*data-storage-directory-for-intelligent-integrated-management-database*

Specifies the absolute-path directory on the shared disk of the cluster environment where Intelligent Integrated Management Database for Logical host is stored.

- In Windows

  Specify a character string of up to 100 single-byte alphanumeric characters, including "_" (underscore), "\", "(", ")", and "." (period), and single-byte spaces.

- In Linux

  Specify a character string of up to 100 single-byte alphanumeric characters, including "_" (underscore), "/" (slash), and "." (period).

During setup, a directory with `imgndb+`*logical-host-number* is created directly under the specified directory, and Intelligent Integrated Management Database is constructed. If you have already built Intelligent Integrated Management Database, you cannot change it from the specification at the time of the build.

There is no default value. This specification is not optional.

`IMGNDBENVDIR=`*directory-where-intelligent-integrated-management-database-is-installed*

Specifies the absolute-path directory on the local disk where you want to install Intelligent Integrated Management Database for Logical host. Do not specify a shared disk in a clustered environment.

- In Windows

  Specify a character string of up to 200 single-byte alphanumeric characters, including "_" (underscore), "\", "(", ")", and "." (period), and single-byte spaces.
- In Linux

  Specify a character string of up to 200 single-byte alphanumeric characters, including "_" (underscore), "/" (slash), and "." (period).

When setting up, create a directory of `imgndbbin`+*logical-host-number* directly under the specified directory, and extract Intelligent Integrated Management Database. If you have already built Intelligent Integrated Management Database, you cannot change it from the specification at the time of the build.

The defaults are following:

In Windows: *Manager-path*`\dbms`

In Linux: `/var/opt/jp1imm/dbms`

If omitted, the default value is assumed.

`LOGICALHOSTNUMBER=`*logical-host-number*

Specifies the number to identify Logical host in Intelligent Integrated Management Database for logical host as a one-byte number from 1 to 9.

If you are adding a logical host, you cannot specify the same number as a number that already exists.

Specify the same number for the execution system and the standby system.

If you have already built Intelligent Integrated Management Database, you cannot change it from the specification at the time of the build.

There is no default value. This specification is not optional.

`RETENTION=`*retention-period-of-time-series-data-in-trend-data-management-DB*

Specify the retention period (unit: days) of the data stored in the trend data management DB.

The range is 1 to 1096.

The default is 32. If omitted, the default value is assumed.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. In a logical host environment, the service remains stopped rather than restarted due to command extensions, so you must manually start the service after running the command.

`USERNAME=`*user-name-of-OS-used-to-start-intelligent-integrated-management-database*

Specifies OS username under which Intelligent Integrated Management Database is launched in Linux, that is, the user who actually exists for a user other than root and who can login it. If specified in Windows configuration, it is ignored.

There is no default value. This specification is not optional.

If you want to change the setting during operation, change this value and run the jimgndbsetup command. In a logical host environment, the service remains stopped rather than restarted due to command extensions, so you must manually start the service after running the command.

`TDDBDISKMAX=`*max-disk-requirements-of-trend-data-management-database*

Specifies the upper limit (in gigabytes) of the disk space required for Trend data Management Database. Automatic Delete occurs when Trend data Management Database disk requirements exceed 90% of this Value. If 0 is specified, the upper limit is not Setup.

The range is 0 or 10 to 131,072.

The default is 150. If the specification is omitted, the default value is assumed.

If you want to change setup during operation, change this value and execute `jimgndbsetup` command. Restart the service with the extension of the command. It will be reflected.

Notes

When using Monitoring Trend data Management Database Disk Requirements feature, we recommend that you specify a value that exceeds the 10-day data size of the trend data stored in Trend data Management Database.

`TDDBCUTOFFTERM=`*truncation-duration-when-trend-data-is-deleted*

Specifies the duration (in days) of the trend data to delete when Trend data Management Database disc requirements reach 90% of the size specified for `TDDBDISKMAX`. If `TDDBDISKMAX` is 0, this field is ignored.

The range is 1 to 31.

The default is 7. If the specification is omitted, the default value is assumed.

If you want to change setup during operation, change this value and execute `jimgndbsetup` command. Restart the service with the extension of the command. It will be reflected.

Example definition

- In Windows

```
#IM DATABASE SERVICE - Logical Host Number
LOGICALHOSTNUMBER=1
#IM DATABASE SERVICE - Logical Host Name
LOGICALHOSTNAME=
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=5433
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=5434
#IM DATABASE SERVICE - Data Storage Directory (Shared Data Area)
SHAREGNDBDIR=S:\share\JP1IMM\gndb
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=C:\Program Files (x86)\Hitachi\JP1IMM\dbms
# IM GNDATABASE SERVICE - Retention
RETENTION=32
# TREND DATA DATABASE - MAX DISK SIZE [GB]
TDDBDISKMAX=764
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=7
```

- In Linux

```
#IM DATABASE SERVICE - Logical Host Number
LOGICALHOSTNUMBER=1
#IM DATABASE SERVICE - Logical Host Name
LOGICALHOSTNAME=
#IM GNDATABASE SERVICE - Port Number
IMGNDBPORT=5433
#TREND DATA MANEGEMENT SERVICE - Port Number
TDMSPORT=5434
#IM DATABASE SERVICE - Data Storage Directory (Shared Data Area)
SHAREGNDBDIR=/share/jp1imm/gndb
#IM GNDATABASE SERVICE - Data Base Binary
IMGNDBENVDIR=/var/opt/jp1imm/dbms
# IM GNDATABASE SERVICE - Retention
RETENTION=32
# IM GNDATABASE SERVICE - Username
USERNAME=USER01
# TREND DATA DATABASE - MAX DISK SIZE [GB]
TDDBDISKMAX=764
```

```
# TREND DATA DATABASE - CUT-OFF TERM [Days]
TDDBCUTOFFTERM=7
```

Intelligent Integrated Management Database configuration file (postgresql.conf)

Format

```
parameter = settings-in-JP1/IM - Manager
parameter = settings-in-JP1/IM - Manager
  :
parameter = settings-in-JP1/IM - Manager
```

File

`postgresql.conf`

`postgresql.conf.model` (model file)

Storage directory

In Windows:

- For a physical host
  Manager-path`\conf\imgndb\`
- For a logical host
  shared-folder`#\jp1imm\conf\imgndb\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imgndb/`
- For a logical host
  shared-directory`#/jp1imm/conf/imgndb/`

#:

JP1/IM - Directory on the shared disk specified when building the Manager's logical host environment (directory specified separately for each logical host)

Description

This file describes parameter definitions related to the Intelligent Integrated Management Database (PostgreSQL).

When the definitions are applied

If you change the parameter settings, you must restart the Intelligent Integrated Management database.

In addition, some parameters are automatically populated when the Intelligent Integrated Administration database is set up to match the resource status of the operating environment.

Information that is specified

parameter = settings-in-JP1/IM - Manager

The parameters that can be set are the same as those provided by PostgreSQL.

The parameters that can be edited by the user are listed in the following table:

Parameter	Type	Description	Settings in JP1/IM - Manager
authentication_timeout	integer	Sets the maximum time to complete client authentication. This parameter can only be set in the postgresql.conf file or on the server command line.	1min
log_filename	string	If logging_collector parameter is in effect, sets the file name of the log file created. This parameter can only be set in the postgresql.conf file or on the server command line.	'postgresql-%a.log'
log_rotation_age	integer	If the logging_collector parameter is in effect, sets the maximum time to use individual log files. This parameter can only be set in the postgresql.conf file or on the server command line.	1d
log_rotation_size	integer	If logging_collector parameter is in effect, sets the maximum size of an individual log file. This parameter can only be set in the postgresql.conf file or on the server command line.	--
log_min_messages	enum	Sets the level of messages written to the server log.	warning
log_min_error_stateme nt	enum	Set whether SQL statements that cause error conditions are recorded in the server log.	error
log_line_prefix	string	Sets the printf-style string that is output at the beginning of each log line.	'%m [%p] %e'
lc_messages	string	Sets the language in which the message is displayed.	'C'
lc_monetary	string	Use the to_char family of functions to set the locale used to format amounts.	'C'
lc_numeric	string	Use the to_char family of functions to set the locale used to format numbers.	'C'
lc_time	string	Use the to_char family of functions to set the locale used to format dates and times.	'C'

Legend:

--: Do not use JP1/IM - Manager.

Item file

Format

```
[@]item-name
# comment-line
    :
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file specifies the JP1 event attributes that are to be output during output of event reports.

The maximum size of this file is 32 kilobytes (32,768 bytes).

Definition specification

- A line consisting of only single-byte spaces or tabs is ignored.
- Single-byte spaces and tabs before the first parameter name on each line, and at the end of each line are ignored.

When the definitions are applied

When the `jcoevtreport` command with the `-k` option specified is executed, the specified item file is loaded and the attribute values of JP1 events are output to event reports according to the item file.

Contents of the file

item-name

Specifies the items you want to output in an event report.

The following table lists and describes the items you can specify.

No.	Specifiable item	Description
1	`B.SEQNO`	Serial number
2	`B.ID`	Event ID
3	`B.PROCESSID`	Source process ID
4	`B.TIME`	Registered time
5	`B.ARRIVEDTIME`	Arrived time
6	`B.REASON`	Reason for registration
7	`B.USERID`	Source user ID

No.	Specifiable item	Description
8	B.GROUPID	Source group ID
9	B.USERNAME	Source user name
10	B.GROUPNAME	Source group name
11	B.SOURCESERVER	Source host
12	B.DESTSERVER	Target event server name
13	B.SOURCEIPADDR	Source IP address
14	B.DESTIPADDR	Target IP address
15	B.SOURCESEQNO	Source event database sequence number
16	B.CODESET	Code set
17	B.MESSAGE	Message
18	E.SEVERITY	Event level
19	E.USER_NAME	User name
20	E.PRODUCT_NAME	Product name
21	E.OBJECT_TYPE	Object type
22	E.OBJECT_NAME	Object name
23	E.ROOT_OBJECT_TYPE	Root object type
24	E.ROOT_OBJECT_NAME	Root object name
25	E.OBJECT_ID	Object ID
26	E.OCCURRENCE	Occurrence
27	E.START_TIME	Start time
28	E.END_TIME	End time
29	E.RESULT_CODE	Return code
30	E.JP1_SOURCEHOST	Event source host name
31	E.@JP1IM_ACTTYPE	Action type
32	E.@JP1IM_ACTCONTROL	Action
33	E.@JP1IM_SEVERE	Severe event
34	E.@JP1IM_CORRELATE	Correlation event
35	E.@JP1IM_RESPONSE	Response waiting event
36	E.@JP1IM_ORIGINAL_SEVERITY	Original severity level
37	E.@JP1IM_CHANGE_SEVERITY	New severity level
38	E.@JP1IM_DEALT	Event status
39	E.@JP1IM_RELEASE	Canceling severe events
40	E.@JP1IM_DISMISSED	Severe event deleted
41	E.@JP1IM_MEMO	Memo
42	E.@JP1IM_DISPLAY_MESSAGE	Changed display message

No.	Specifiable item	Description
43	`E.@JP1IM_CHANGE_MESSAGE`	New display message
44	`E.@JP1IM_CHANGE_MESSAGE_NAME`	Display message change definition
45	`E.`*user-specific extended attribute*	Extended attribute

If there is no corresponding attribute in a JP1 event, the null character is output.

In addition, if you specify `@` at the beginning of an item name, the date and time item for the basic or extended attribute is output, in the format *YYYYMMDDhhmmss*.

However, if any of the attributes of a JP1 event contain any of the following values, the value of the date and time item is output as is, even if `@` is specified.

- nonnumeric value
- value less than 0, or value greater than 4,102,444,800

`#`*comment-line*

A line beginning with a hash mark (`#`) is treated as a comment.

Example definition

```
B.SEQNO
B.ID
B.PROCESSID
B.TIME
  :
```

Environment definition file for event report output (evtreport.conf)

Format

```
[logical-host-name\JP1CONSOLEMANAGER]
"PROGRAM_SPECIFIC_EX_ATTR_COLUMN"=dword:hexadecimal-value
```

File

`evtreport.conf.update` (model file for the environment definition file for event report output)

Storage directory

In Windows

Console-path`\default\`

In UNIX

`/etc/opt/jp1cons/default/`

Description

This file defines the execution environment of the event report output function. It specifies whether to enable the function.

The required definitions are provided as a model file. To change the settings, copy the model file and edit the copy after renaming the copy to definition file (for Windows: *console-path*`\conf\evtreport.conf`, for UNIX: `/etc/opt/jp1cons/conf/evtreport.conf`).

When the definitions are applied

The definitions take effect when JP1/IM - Manager is restarted after the `jbssetcnf` command has been executed in JP1/Base to apply the definitions to the JP1 common definition information.

Information that is specified

`[`*logical-host-name*`\JP1CONSOLEMANAGER]`

Indicates the key name of the JP1/IM - Manager environment settings.

For *logical-host-name*, specify `JP1_DEFAULT` for a physical host and *logical-host-name* for a logical host.

`"PROGRAM_SPECIFIC_EX_ATTR_COLUMN"=dword:`*hexadecimal-value*

Specifies whether to enable the function for assigning a column to each program-specific extended attribute function when program-specific extended attributes are output using the `jcoevtreport` command, in the same way as for basic attributes, common extended attributes, and IM attributes.

- `00000001`: Enable
- `00000000`: Disable

The default value is `00000001` (enable).

Example definition

```
[JP1_DEFAULT\JP1CONSOLEMANAGER]
"PROGRAM_SPECIFIC_EX_ATTR_COLUMN"=dword:00000001
```

Filter file

Format

```
event-condition
     :
OR
event-condition
     :
EXCLUDE
event-condition
     :
```

File

Use any file.

Storage directory

In Windows

Any folder

In UNIX

Any directory

Description

This file defines filter conditions to be applied during output of event reports. To load the file, execute the `jcoevtreport` command with the `-f` option specified.

The maximum size of this file is 256 kilobytes (262,144 bytes).

When the definitions are applied

When the `jcoevtreport` command with the `-f` option specified is executed, the specified item file is loaded and the JP1 events that satisfy the specified condition are acquired from the integrated monitoring database and then output to an event report.

Contents of the file

pass-conditions group, exclusion-conditions group

The `jcoevtreport` command outputs the JP1 events that do not satisfy any of the exclusion-conditions groups and that satisfy one of the pass-conditions groups. For the filter conditions, you can specify from 0 to 5 pass-conditions groups and from 0 to 5 exclusion-conditions groups.

In a pass-conditions group or exclusion-conditions group, you can specify from 0 to 50 event conditions. In the case of an extended attribute (user-specific information), you can specify a maximum of 5 event conditions per pass-conditions group or exclusion-conditions group.

`OR`

If you specify multiple condition groups, specify `OR` between the condition groups.

`EXCLUDE`

Specify `EXCLUDE` between a pass-conditions group and an exclusion-conditions group. Any event condition that follows `EXCLUDE` is treated as an exclusion-conditions group. If no event condition follows `EXCLUDE`, only the pass-conditions groups take effect.

event-condition

Specify the event conditions in the following format (Δ indicates a single-byte space):

*attribute-name*Δ*comparison-keyword*Δ *operand*`[`Δ*operand*`] ...`

Note that a line consisting of only spaces or tabs is ignored during processing.

attribute-name

Specifies the name of the attribute that you want to compare. To specify a basic attribute, place `B.` immediately before the name; to specify an extended attribute (common information or user-specific information), place `E.` immediately before the name. Attribute names are case sensitive.

comparison-keyword

Specifies one of `BEGIN` (begins with), `IN` (matches), `NOTIN` (does not match), `SUBSTR` (includes), `NOTSUBSTR` (does not include), or `REGEX` (regular expression) as the comparison keyword. The comparison keyword is case sensitive.

operand

Specifies a character string as the value that is to be compared with the attribute value by the specified comparison keyword. Operands are case sensitive.

Specify multiple operands by separating them with one or more consecutive spaces or a tab. The OR condition is applied to the specified operands. Note that if a regular expression is specified for the comparison keyword, only one operand can be specified.

To specify a space, a tab, end-of-line code (CR or LF), or % as a part of an operand, specify as follows:

No.	Value to be specified	How to specify
1	Tab (`0x09`)	`%09`
2	Space (`0x20`)	`%20`
3	`%` (`0x25`)	`%25`
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.IDΔINΔ100Δ200`

Legend:

Δ: Space (`0x20`)

You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length of operands in bytes that are specified in the event condition block). The following table shows the attribute names, comparison keywords, and operands that can be specified for event conditions.

No.	Item	Attribute name	Comparison keyword	Operand
1	Event ID	`B.ID`	• `Match` • `Does not match`	• A maximum of 100 event IDs can be specified. • Event IDs are not case sensitive. • The permitted range is from `0` to `7FFFFFFF`.

No.	Item	Attribute name	Comparison keyword	Operand
2	Reason for registration	`B.REASON`	• `Match` • `Does not match`	• A maximum of 100 items can be specified. • The permitted range is from -2,147,483,648 to 2,147,483,647.
3	Source process ID	`B.PROCESSID`		
4	Source user ID	`B.USERID`		
5	Source group ID	`B.GROUPID`	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	• A maximum of 100 items can be specified. However, if a regular expression is specified, only one item is allowed.
6	Source user name	`B.USERNAME`		
7	Source group name	`B.GROUPNAME`		
8	Event-issuing server name#1	`B.SOURCESERVER`		
9	Target event server name#1	`B.DESTSERVER`		
10	Message	`B.MESSAGE`		
11	Event level	`E.SEVERITY`	`Match`	• Specifiable values are `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, and `Debug`. • Multiple event levels can be specified. However, the same event level cannot be specified twice.
12	Extended attribute#2	`E.`*xxxxxxx*	• `First characters` • `Match` • `Does not match` • `Is contained` • `Is not contained` • `Regular expression`	• For the extended attribute name, you can specify a character string with a maximum of 32 bytes that begins with an uppercase letter and consists of uppercase letters, numeric characters, and the underscore (_). • A maximum of 100 extended attributes can be specified. However, if a regular expression is specified, only one extended attribute is allowed.
13	Action type	`E.@JP1IM_ACTTYPE`	• `Match` • `Does not match`	• The following numeric values can be specified: `0`: Not subject to an action `1`: Command • Multiple action types can be specified.
14	Action suppression	`E.@JP1IM_ACTCONTROL`		• The following numeric values can be specified: `0`: Not subject to an action 1: Execution 2: Suppression

No.	Item	Attribute name	Comparison keyword	Operand
				3: Partial suppression - Multiple action suppressions can be specified.
15	Severe event	E.@JP1IM_SEVERE		- The following numeric values can be specified: 0: Not a severe event 1: Severe event - Multiple severe events can be specified.
16	Correlation event	E.@JP1IM_CORRELATE		- The following numeric values can be specified: 0: Not a correlation event 1: Correlation approval event 2: Correlation failure event - Multiple correlation events can be specified.
17	Response waiting event	E.@JP1IM_RESPONSE		- The following numeric values can be specified: 0: Not a response waiting event 1: Response waiting event - Multiple response waiting events can be specified.
18	Original severity level	E.@JP1IM_ORIGINAL_SEVERITY	- First characters - Match - Does not match - Is contained - Is not contained - Regular expression	- Multiple original severity levels can be specified. A maximum of 100 original severity levels can be specified. However, if a regular expression is specified, only one level is allowed.
19	New severity level	E.@JP1IM_CHANGE_SEVERITY	- Match - Does not match	- The following numeric values can be specified: 0: No new severity level exists 1: New severity level exists - Multiple new severity levels can be specified.
20	Event status	E.@JP1IM_DEALT		- The following numeric values can be specified: 0: Not processed 1: Already processed 2: Being processed 3: On hold - Multiple event statuses can be specified.
21	Severe event released	E.@JP1IM_RELEASE		- The following numeric values can be specified: 0: No severe events are released 1: Severe events are released - This item can be specified multiple times.
22	Severe event deleted	E.@JP1IM_DISMISSED		- The following numeric values can be specified: 0: No severe events are deleted 1: Severe events are deleted - This item can be specified multiple times.
23	Memo	E.@JP1IM_MEMO	- First characters - Match	- A maximum of 100 memos can be specified. However, if a regular expression is specified, only one memo is allowed.

No.	Item	Attribute name	Comparison keyword	Operand
			• Does not match • Is contained • Is not contained • Regular expression	
24	Changed display message#3	E.@JP1IM_DISPLAY_MESSAGE	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	• A maximum of 100 of these items can be specified. However, if a regular expression is specified, only one item is allowed.
25	New display message#3	E.@JP1IM_CHANGE_MESSAGE	• Match • Does not match	• The permitted range is from -2,147,483,648 to 2,147,483,647.
26	Display message change definition #3	E.@JP1IM_CHANGE_MESSAGE_NAME	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	• A maximum of 100 of these items can be specified. However, if a regular expression is specified, only one item is allowed.
27	Event source host name#2	E.JP1_SOURCEHOST	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	• A maximum of 100 of these items can be specified. However, if a regular expression is specified, only one item is allowed.

#1

If the integrated monitoring database and the IM Configuration Management database are enabled, and the comparison keyword is Match or Do not match, you can specify the business group name in a path format.

If the integrated monitoring database and the IM Configuration Management database are disabled, and a comparison keyword other than Match and Do not match is selected, a business group name specified in a path format is treated as a host name.

If the -ignorecasehost option of the jcoimdef command is set to ON, and a comparison keyword other than Regular expression is selected, the character string is no longer case sensitive.

#2

E.START_TIME (start time), and E.END_TIME (end time) cannot be specified.

#3

If you have upgraded from version 10-50 or earlier of JP1/IM - Manager, this item is not output unless the integrated monitoring database has been updated using the jimdbupdate command.

Example definition

```
B.ID IN 1
B.MESSAGE SUBSTR Warning
E.SOURCESERVER IN host1 host2 host3 host4
OR
B.ID IN 1
B.MESSAGE SUBSTR Error
E.SOURCESERVER IN host1 host2 host3 host4
EXCLUDE
E.SOURCESERVER IN host3
```

Details of statements in definition files

This subsection lists the types and structures of and the values that can be specified in the statements that can be specified in some of the JP1/IM definition files.

Note:

The information provided in this subsection is applicable only to the following three definition files:

- Definition file for extended event attributes
- Definition file for executing applications
- Definition file for the Tool Launcher window

Types of statements

Table 2–91: Types of statements

Statement category	Statement types
In-file statements	Start-of-block statement End-of-block statement File attribute statement Product statement
In-block statements	Definition statement for function menu command options Event attribute definition statement Block attribute definition statement Definition file for function menu execution definition identifiers Application description definition statement Group definition statement Function menu display icon definition statement Definition statement for application execution definition identifiers Function menu identifier definition statement Function menu display name definition statement Sequence definition statement Function menu parent identifier definition statement Application path definition statement

Structures of statements

Table 2–92: Structures of statements

Statement type	Specification format
Start-of-block statement	`@define-block type=`*block-type*
End-of-block statement	`@define-block-end`
File attribute statement	`@file type=`*definition-file-type*`[, version=`*definition-format-version*`]`
Product statement	`@product name=`*product-name*
Definition statement for function menu command options	`arguments=`*command-arguments*
Event attribute definition statement	`attr name=`*attribute-name*`, title=`*display-item-name*`[, type=`*attribute-display-type*`]`

Statement type	Specification format
Block attribute definition statement	`block lang=`*language-type*`|platform=`*platform-type*`|version=`*version-in-use*
Definition file for function menu execution definition identifiers	`execute_id=`*application-execution-definition-identifier*
Application description definition statement	`description=`*description-of-application-execution*
Group definition statement	`group name=`*group-name*`, attrs=`*list-of-attribute-names*
Function menu display icon definition statement	`icon=`*display-icon-file-name*
Definition statement for application execution definition identifiers	`id=`*application-execution-definition-identifier*
Function menu identifier definition statement	`id=`*function-menu-identifier*
Function menu display name definition statement	`name=`*display-name*
Sequence definition statement	`order id=`*event-ID-definition-character-string*`, attrs=`*list-of-attribute-names*
Function menu parent identifier definition statement	`parent_id=`*parent-function-menu-identifier*
Application path definition statement	`path=`*command-path*

Rules for generating specification components in the statements

The table below lists the values that can be specified in the specification components of the statements.

Table 2–93: Values that can be specified in the specification components of the statements

Specification components	Specifiable values
Hexadecimal characters	From `0` to `9` and `A` to `F`
EUCJIS	EUCJIS
GB18030	GB18030
JIS	JIS
Shift-JIS	SJIS
UTF-8	UTF-8
Description of application execution	User-defined character string of from 1 to 50 bytes
Application execution definition	`application-execution-definition`
Application execution definition block	`application-execution-def`
Application execution definition identifier	From 1 to 32 alphanumeric characters
Event ID	From 1 to 8 bytes of hexadecimal characters
Event ID definition character string	*event-ID* `|` *event-ID-definition-character-string enumeration-separator event-ID*
Event object type definition block	`event-object-def`
Event extended attribute definition	`extended-attributes-definition`
Event attribute group definition block	`event-attr-group-def`
Event attribute definition block	`event-attr-def`
Event display sequence definition block	`event-attr-order-def`

Specification components	Specifiable values
Interface name	From 1 to 32 alphanumeric characters
Group name	From 1 to 32 alphanumeric characters
Command path	File name
Command arguments	User-defined character string that serves as command arguments
Subkey name	From 1 to 32 alphanumeric characters
Forward slash	`/`
Forward slash-separated alphanumeric character string	*forward-slash* | *alphanumeric-characters* | *forward-slash-separated-alphanumeric-character-string forward-slash* | *forward-slash-separated-alphanumeric-character-string alphanumeric-characters*
Default	`default`
Version	Version character string expressed using from 1 to 7 alphanumeric characters
Version symbolic character	`/|.|-`
Version range specification	*version space−space version*
Version character	*uppercase-letters* | *number* | *version-symbolic-character*
File symbolic character	`.|/|\\\|-|_|~`
File name	Character string that serves as a file path
File name character string	*file-symbolic-characters* | *alphanumeric characters* | *file-name-character-string file-symbolic-characters* | *file-name-character-string alphanumeric-characters*
Platform type	`base` | *alphanumeric-character-string*
Product name	Forward slash-separated alphanumeric character string
Block type	*event-attribute-definition-block* | *event-attribute-group-definition-block* | *event-display-sequence-definition-block* | *application-execution-definition-block*
User-defined character	*alphanumeric-character* | *Japanese-characters* | *symbol*
English	`English`
Alphabetic characters	Uppercase and lowercase alphabetic characters
Lowercase letters	From `a` to `z`
Alphanumeric characters	Alphabetic and numeric characters
Uppercase letters	From `A` to `Z`
Menu tree node definition block	`function-tree-def`
Integrated tree menu definition	`function-definition`
Function menu identifier	From 1 to 32 alphanumeric characters
Function menu identifier string	`[`*from-0-to-9-bytes-of-function-menu-identifier enumeration-separator*`]` *function-menu-identifier*
Language type	Japanese | English
Parent function menu identifier	Function menu identifier
Numeric characters	From `0` to `9`
Description	From 1 to 50 bytes of user-defined characters

Specification components	Specifiable values
Attribute value	From 1 to 10,000 bytes of characters
Attribute value type	`elapsed_time`
Attribute display type	*attribute-value-type* / *display-format*
Attribute name	`(B|).`*attribute-name-character-string*
Attribute name characters	*uppercase-letters* | *numeric-characters* | _
Attribute name character string	Attribute name characters consisting of from 0 to 31 uppercase letters
Attribute name list	*attribute-name* | *list-of-attribute-names*`\` | *attribute-names*
Definition file type	*extended-event-attribute-definition* | *application-execution-definition* | *definition-for-opening-monitor-windows* | *Tool-Launcher-definition*
Definition format version	`0300`
Supported version	`ALL` | *version* | *version-range-specification*
Date and time display format	`date_format:`*display-time-zone*
Japanese	Japanese
Japanese characters	Two-byte characters except one-byte kana
Japanese character encoding	Shift-JIS | EUCJIS | JIS | UTF-8
Display icon file name	*file-name*
Display time zone	`CLIENT`
Display format	Date and time display format
Display item character	*alphanumeric-characters* | *space* | `-` | `_` | *Japanese-characters*
Display item character string	From 0 to 64 bytes of display item character string
Display item name	Display item character string
Display name	From 1 to 32 bytes of user-defined character string
Enumeration separator	`\\|`

Node exporter metric definition file (metrics_node_exporter.conf)

Format

```
[
  {
    "name":"trend-data-metric-names",
    "default":default-selection-state,
    "promql":"PromQL-statement",
    "resource_en":{
      "category":"metric-category-(English)",
      "label":"metric-display-name-(English)",
      "description":"metric-description-(English)",
      "unit":"metric-unit-(English)"
    },
    "resource_ja":{
      "category":"metric-category-(Japanese)",
      "label":"metric-display-name-(Japanese)",
      "description":"metric-description-(Japanese)",
      "unit":"metric-unit-(Japanese)"
    },
    "drop_legend_labels": ["label-name", ...]
  }, ...
]#
```

#

The number of elements that can be described in `[]` is 1 to 1,000. If an out-of-range number of elements is described, a KAJY24609-E error message is output.

File

`metrics_node_exporter.conf`

`metrics_node_exporter.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines the metric information for the Node exporter to be displayed on the **Trend** tab of the Unified Operations Viewer screen.

The defined contents are used for the return values of __metricListGet method and __timeSeriesDataGet method of the JP1/IM - Agent product plug-in.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

It is reflected when metric information is obtained on the **Trend** tab of the Integrated Operation Viewer screen or with the REST API.

Information that is specified

Table 2–94: Values to set for each member of the metrics definition file

Member name	Optional	Type	Value to set
name	No	string	Set trend data metric names. The metric name of trend data (time series data) is displayed as a character string indicating the type of trend data on the Trend tab of the Unified Operation Viewer screen. 1 to 255 characters, and the following characters can be specified. • Single-byte alphanumeric characters • - (hyphen) • _ (underscore) If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. The metric name must be unique within the metric definition file. Otherwise, a KAJY24608-E error message is output.
default	Yes	boolean	Set default selection state. Specifies whether the check box of trend data selected on the Trend tab of the Integrated Operation Viewer screen is selected by default. • true: Checked by default. • false: Unchecked by default. If it is omitted, it is not checked by default.
promql	No	string	Set PromQL statement. You can configure PromQL statements that can be used in JP1/IM trend data reference API.

Member name	Optional	Type	Value to set
			The string "$jp1im_TrendData_labels" in the PromQL statement is replaced by the PromQL statement described in "■*Replacing $jp1im_TrendData_labels*" below. For notes on PromQL statements, see *Note on PromQL expression*. Specify 1 to 1,023 characters except control characters (0x00~0x1F, 0x7F~0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed.
resource_en	No	object	Configure resource information for metrics.
category	Yes	string	Set the category of the metric. Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. The default is not to set the metric category.
label	Yes	string	Set the display name of the metric. Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. By default, the settings of the name member are used for the display name of the metric on the Trends tab of the Unified Operations Viewer screen. Also, the display name of the metric is not returned by the metric list acquisition API.
description	Yes	string	Sets the description of the metric. Specifies 1 to 1,023 characters, excluding control characters (0x00 to 0x1F,0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. By default, metric descriptions are not displayed on the Trends tab of the Unified Operations Viewer screen. Also, the metric description is not returned by the metric list acquisition API.
unit	No	string	Set the units for the metric. Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed.
resource_ja	Yes	object	Set the resource information (Japanese) for the metric. By default, the resource_en settings are used.
category	Yes	string	Set the category of the metric (Japanese). Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. By default, the settings of the resource_en category are used.
label	Yes	string	Set the display name (Japanese) of the metric. Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. If it is the default, the label setting of the resource_en is used.

Member name	Optional	Type	Value to set
description	Yes	string	Set the description of the metric (Japanese). Specifies 1 to 1,023 characters, excluding control characters (0x00 to 0x1F,0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. By default, the description setting of the resource_en is used.
unit	Yes	string	Set the unit of the metric (Japanese). Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. By default, the settings of the resource_en unit are used.
drop_legend_labels	Yes	Array (string)	Set the label name if you want to add a label that you want to exclude from the trend chart legend. In addition to the labels to be excluded shown in *3.15.6(4)(b) Instance name (a string to display as a legend in the graph)* of the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*, the names of labels to be excluded from the legend of the trend graph are described. Specify 1 to 255 characters except control characters (0x00 to 0x1F, 0x7F to 0x9F). If it contains characters that cannot be specified, it is not excluded from the legend of the trend graph. You can specify up to 100 labels. If there are more than 100 labels, the 101st and subsequent labels are ignored.

■Replacing $jp1im_TrendData_labels

The string "$jp1im_TrendData_labels" in the promql value is replaced with a PromQL statement to narrow down the target of retrieval when retrieving performance data.

The following is the replaced PromQL statement for each SID type of configuration information specified in the Trending API or Unified Operations Viewer (for CloudWatchSIDs other than EC2, for each monitored AWS namespace). The bold part (variable value) is replaced by the Exporter setting managed by the corresponding SID or the sample value output by the Exporter.

Table 2–95: PromQL statement after replacing $jp1im_TrendData_labels

Configuration information SID type	PromQL statement after replacement
Agent SID	`{jp1_pc_prome_hostname="`*Prometheus-host-name*`",job="`*scrape-job-name*`",instance="`*value-of-instance-label*`"}`
Remote agent SID	
CloudWatchSID of EC2	`{jp1_pc_prome_hostname="`*Prometheus-host-name*`",job="`*scrape-job-name*`",instance="`*value-of-instance-label*`"},jp1_pc_nodelabel="`*The value that you set for the jp1_pc_nodelabel tag of the resource in AWS*`"}`
CloudWatchSID other than EC2	

Model file settings (initial state)

The setting contents (initial state) of each metric described in the model file of the Node exporter metric definition file are shown below.

- cpu_used_rate#

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		cpu_used_rate
default		true
The promql for metric definition File (including $jp1im_TrendData_labels)		(avg by (instance,job,jp1_pc_nodelabel,jp1_pc_prome_hostname) (rate(node_cpu_seconds_total{mode=\"system\"}[2m]) and $jp1im_TrendData_labels) + avg by (instance,job,jp1_pc_nodelabel,jp1_pc_prome_hostname) (rate(node_cpu_seconds_total{mode=\"user\"}[2m]) and $jp1im_TrendData_labels)) * 100
resource_en	category	platform_unix
	label	CPU used rate
	description	CPU usage.It also indicates the average value per processor. [Units: %]
	unit	%
resource_ja	category	platform_unix
	label	CPU 使用率
	description	CPU 使用率（%）。 プロセッサごとの割合の平均値でもある。
	unit	%

#

Equivalent to the CPU % field in the PI record of JP1/PFM - Agent for Platform (Unix).

- memory_unused#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		memory_unused
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(node_memory_MemAvailable_bytes and $jp1im_TrendData_labels)/1024/1024/1024
resource_en	category	platform_unix
	label	Memory unused
	description	Size of the physical memory that can actually be used by the application.
	unit	GB
resource_ja	category	platform_unix
	label	空きメモリ量
	description	実際にアプリケーションが使用することができる物理メモリーのサイズ。
	unit	ギガバイト

#

Equivalent to the Effective Free Mem Mbytes field in the PI record of JP1/PFM - Agent for Platform (Unix). However, the number unit are different.

- memory_unused_rate#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		memory_unused_rate
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(node_memory_MemAvailable_bytes and $jp1im_TrendData_labels) / (node_memory_MemTotal_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	platform_unix
	label	Available memory percentage
	description	Percentage of physical memory actually available to the application
	unit	%
resource_ja	category	platform_unix
	label	空きメモリ率
	description	実際にアプリケーションが使用することができる物理メモリーの割合。
	unit	%

#

Equivalent to Effective Free Mem % field in PI record of JP1/PFM - Agent for Platform (Unix).

- disk_unused#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_unused
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(node_filesystem_free_bytes and $jp1im_TrendData_labels)/(1024*1024*1024)
resource_en	category	platform_unix
	label	Disk unused
	description	Size of the unused area of the disk. [Units: GB]
	unit	GB
resource_ja	category	platform_unix
	label	空きディスク領域
	description	ディスクの未使用領域のサイズ。（単位:ギガバイト）
	unit	ギガバイト

#

Equivalent to the Mbytes Free field in the PD_FSL record of JP1/PFM - Agent for Platform (Unix). However, the number unit are different.

- disk_unused_rate#

■Configuration contents (default status)

Member name	Configuration contents (default status)
name	disk_unused_rate

Member name		Configuration contents (default status)
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(node_filesystem_free_bytes and $jp1im_TrendData_labels) / (node_filesystem_size_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	platform_unix
	label	Unused disk space percentage
	description	Percentage of unused disk space
	unit	%
resource_ja	category	platform_unix
	label	空きディスク率
	description	ディスクの未使用領域の割合。
	unit	%

#

Equivalent to Mbytes Free % field of the PD_FSL record in JP1/PFM - Agent for Platform (Unix).

- disk_busy_rate#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_busy_rate
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(node_disk_io_time_seconds_total[2m]) and $jp1im_TrendData_labels)*100
resource_en	category	platform_unix
	label	Disk busy rate
	description	Percentage of time the disk was busy with read and write requests. This value may exceed 100 when processes are continuously executed on a device. [Units: %]
	unit	%
resource_ja	category	platform_unix
	label	ディスクビジー率
	description	ディスクのビジー率（%）。 デバイスに対する処理が連続で行われる場合に「100」を超えることがあります。
	unit	%

#

Equivalent to the Busy % field in the PI_DEVD record of JP1/PFM - Agent for Platform (Unix).

- disk_read_latency

■Configuration contents (default status)

Member name	Configuration contents (default status)
name	disk_read_latency

Member name		Configuration contents (default status)
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(node_disk_read_time_seconds_total[2m]) and $jp1im_TrendData_labels) / (rate(node_disk_reads_completed_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Disk read latency
	description	Average time (in seconds) taken to perform a single disk read operation
	unit	second
resource_ja	category	platform_unix
	label	ディスク読み込みレイテンシー
	description	1 回あたりのディスク読み込みにかかった平均時間（秒）。
	unit	秒

- disk_write_latency

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_write_latency
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(node_disk_write_time_seconds_total[2m]) and $jp1im_TrendData_labels) / (rate(node_disk_writes_completed_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Disk write latency
	description	Average time (in seconds) taken to perform a single disk write operation
	unit	second
resource_ja	category	platform_unix
	label	ディスク書き込みレイテンシー
	description	1 回あたりのディスク書き込みにかかった平均時間（秒）。
	unit	秒

- disk_io_latency

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_io_latency
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		((rate(node_disk_read_time_seconds_total[2m]) and $jp1im_TrendData_labels) + (rate(node_disk_write_time_seconds_total[2m]) and $jp1im_TrendData_labels)) / ((rate(node_disk_reads_completed_total[2m]) and $jp1im_TrendData_labels) + (rate(node_disk_writes_completed_total[2m]) and $jp1im_TrendData_labels))
resource_en	category	platform_unix
	label	Disk I/O latency

Member name		Configuration contents (default status)
	description	Average time (in seconds) taken to perform a single disk write and read operation
	unit	second
resource_ja	category	platform_unix
	label	ディスク IO レイテンシー
	description	1 回あたりのディスク書き込みとディスク読み込みにかかった平均時間（秒）。
	unit	秒

- network_sent#

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		network_sent
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(node_network_transmit_packets_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Network sent
	description	Rate at which packets were sent throughthe network interface. [Units: packets/second]
	unit	packets/second
resource_ja	category	platform_unix
	label	ネットワークの送信速度
	description	ネットワークインターフェースで送信されるパケットの割合。（単位：パケット／秒）
	unit	パケット／秒

#

Equivalent to the Pkts Xmitd/sec field in the PI_NIND record of JP1/PFM - Agent for Platform (Unix).

- network_received#

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		network_received
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(node_network_receive_packets_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Network received
	description	Rate at which packets were receivedthrough the network interface. [Units: packets/second]
	unit	packets/second

Member name		Configuration contents (default status)
resource_ja	category	platform_unix
	label	ネットワークの受信速度
	description	ネットワークインターフェースで受信されるパケットの割合。（単位：パケット／秒）
	unit	パケット/秒

#

Equivalent to the Pkts Rcvd/sec field in the PI_NIND record of JP1/PFM - Agent for Platform (Unix).

Process exporter metric definition file (metrics_process_exporter.conf)

Syntax

The same as the JP1/IM - Agent Node exporter metric definition file.

File

`metrics_process_exporter.conf`

`metrics_process_exporter.conf.model` (Model file)

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines Process exporter metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins. If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the **Trends** tab on the Integrated Operation Viewer window, or in the REST API.

Content description

The same as the JP1/IM - Agent Node exporter metric definition file.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the Process exporter metric definition file (model file).

- process_pgm_process_count#

  - Settings (initial status)

Member		Setting (initial status)
name		process_pgm_process_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (namedprocess_namegroup_num_procs and $jp1im_TrendData_labels)
resource_en	category	platform_unix_process
	label	Process count
	description	Number of processes that are executing programs. Number of processes that have this program name inside the process table.
	unit	count

#

This is equivalent to the Start Time Process Count (PROCESS_COUNT) field in the JP1/PFM - Agent for Platform (UNIX) PD_PGM record.

Node exporter (Service monitoring) metric definition file (metrics_node_exporter_service.conf)

Syntax

See *Syntax* in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_node_exporter_service.conf`

`metrics_node_exporter_service.conf.model (model file)`

Storage directory

- Integration Manager host

For Windows

- When using a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- When using a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

- When using a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- When using a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

Used to get the trend with the service monitoring function of Linux. For details about the service monitor feature, see *Specifying monitored services* in *3.15.1(1)(d) Node exporter (Linux performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This definition file defines metric information that can be retrieved by IM management node of the service.

If JP1/IM - Manager is in a hierarchical configuration and you want the Integration Manager to refer to trend data stored in Trend data Management Database of lower manager, you must add the referenced trend data metrics to the Integration Manager metric definition file.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the Trends tab on the Integrated Operation Viewer window, or in the REST API.

Content description

See Content description in Node exporter metric definition file (metrics_node_exporter.conf)in (2. Definition Files) JP1/IM - Agent.

Settings in the model file (initial status)

- service_state#
  - Settings (initial status)

Member		Setting (initial status)
name		service_state
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		node_systemd_unit_state{state=\"active\"} and $jp1im_TrendData_labels
resource_en	category	platform_linux_service
	label	Service state
	description	Shows the state of the service. 0: Indicates that the service is not active. 1: Indicates that the service is active
	unit	-

#

JP1/PFM - Agent for Platform (UNIX) has no applicable fields.

Windows exporter metric definition file (metrics_windows_exporter.conf)

Format

See the *Format* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_windows_exporter.conf`

`metrics_windows_exporter.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines the Windows exporter metric information displayed on the Trends tab of the Integrated Operation Viewer window.

The defined contents are used for the return values of JP1/IM - __metricListGet method and __timeSeriesDataGet method of the agent product plug-in.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

It is reflected when metric information is obtained on the [Trend] tab of the Integrated Operation Viewer window or in the REST API.

Information that is specified

See the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

Model file settings (initial state)

The setting contents (initial state) of each metric described in the model file of the Windows exporter metric definition file are shown below.

- cpu_used_rate#

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		cpu_used_rate
default		true
The promql for metric definition File (including $jp1im_TrendData_labels)		100 - (avg by (instance,job,jp1_pc_nodelabel,jp1_pc_prome_hostname) (rate(windows_cpu_time_total{mode=\"idle\"}[2m]) and $jp1im_TrendData_labels) * 100)
resource_en	category	platform_windows
	label	CPU used rate
	description	Processor usage. Percentage of elapsed time used by the processor for executing non-idle threads. [Units: %]
	unit	%
resource_ja	category	platform_windows
	label	CPU 使用率
	description	プロセッサの使用率。プロセッサが非アイドル状態のスレッドを実行した経過時間の割合。（単位:%）
	unit	%

#

JP1/PFM - Equivalent to the CPU % field in the PI record of the Agent for Platform (Windows).

- memory_unused#

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		memory_unused
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(windows_memory_available_bytes and $jp1im_TrendData_labels) / (1024*1024*1024)
resource_en	category	platform_windows
	label	Memory unused
	description	Available size in the physical memory area. The combined total of zero memory, free memory, and standby memory (cached) that can be immediately allocated to a process or be used by the system. [Units: GB]
	unit	GB
resource_ja	category	platform_windows

Member name		Configuration contents (default status)
	label	空きメモリ量
	description	物理メモリー領域の未使用サイズ。プロセスへの割り当て，またはシステムがすぐに利用できるゼロメモリー，空きメモリー，およびスタンバイメモリー（キャッシュ済み）の領域の合計。（単位:ギガバイト）
	unit	ギガバイト

#

JP1/PFM - Equivalent to the Available Mbytes field in the PI record of the Agent for Platform (Windows). However, the number unit are different.

- memory_unused_rate#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		memory_unused_rate
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(windows_memory_available_bytes and $jp1im_TrendData_labels) / (windows_cs_physical_memory_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	platform_windows
	label	Available memory percentage
	description	Percentage of available physical memory
	unit	%
resource_ja	category	platform_windows
	label	空きメモリ率
	description	物理メモリの空き容量の割合。
	unit	%

#

There are no fields fall under JP1/PFM - Agent for Platform (Windows).

- disk_unused#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_unused
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(windows_logical_disk_free_bytes and $jp1im_TrendData_labels) / (1024*1024*1024)
resource_en	category	platform_windows
	label	Unused disk space percentage
	description	Percentage of unused disk space
	unit	GB
resource_ja	category	platform_windows

Member name		Configuration contents (default status)
	label	空きディスク領域
	description	ディスクの未使用領域のサイズ。（単位:ギガバイト）
	unit	ギガバイト

#

JP1/PFM - Equivalent to the Free Mbytes field in the Agent for Platform (Windows) PI_LOGD record. However, the number unit are different.

- disk_unused_rate#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_unused_rate
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(windows_logical_disk_free_bytes and $jp1im_TrendData_labels) / (windows_logical_disk_size_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	platform_windows
	label	Unused disk space percentage
	description	Percentage of unused disk space
	unit	%
resource_ja	category	platform_windows
	label	空きディスク率
	description	ディスクの未使用領域の割合。
	unit	%

#

Equivalent to the % Free Space field in the PI_LOGD record for JP1/PFM - Agent for Platform (Windows).

- disk_busy_rate#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_busy_rate
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		100 - (rate(windows_logical_disk_idle_seconds_total[2m]) and $jp1im_TrendData_labels)/((rate(windows_logical_disk_write_seconds_total[2m]) and $jp1im_TrendData_labels) + (rate(windows_logical_disk_read_seconds_total[2m]) and $jp1im_TrendData_labels) + (rate(windows_logical_disk_idle_seconds_total[2m]) and $jp1im_TrendData_labels)) * 100
resource_en	category	platform_windows
	label	Disk busy rate
	description	Percentage of time the disk was busy when a read or write request was processed. [Units: %]

Member name		Configuration contents (default status)
	unit	%
resource_ja	category	platform_windows
	label	ディスクビジー率
	description	読み込みおよび書き込み要求の処理でディスクがビジーだった経過時間の割合。（単位:%）
	unit	%

#

JP1/PFM - Equivalent to the % Disk Time field in the Agent for Platform (Windows) PI_PHYD record.

- disk_read_latency#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_read_latency
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(windows_logical_disk_read_seconds_total[2m]) and $jp1im_TrendData_labels) / (rate(windows_logical_disk_reads_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_windows
	label	Disk read latency
	description	Average time (in seconds) taken to perform a single disk read operation
	unit	second
resource_ja	category	platform_windows
	label	ディスク読み込みレイテンシー
	description	1 回あたりのディスク読み込みにかかった平均時間（秒）。
	unit	秒

#

Equivalent to Avg Disk Secs/Read field in the PI_LOGD record in JP1/PFM - Agent for Platform (Windows).

- disk_write_latency#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_write_latency
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(rate(windows_logical_disk_write_seconds_total[2m]) and $jp1im_TrendData_labels) / (rate(windows_logical_disk_writes_total[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_windows
	label	Disk write latency
	description	Average time (in seconds) taken to perform a single disk write operation

Member name		Configuration contents (default status)
	unit	second
resource_ja	category	platform_windows
	label	ディスク書き込みレイテンシー
	description	1 回あたりのディスク書き込みにかかった平均時間（秒）。
	unit	秒

#

Equivalent to Avg Disk Secs/Write field in the PI_LOGD record in JP1/PFM - Agent for Platform (Windows).

- disk_io_latency#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		disk_io_latency
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		((rate(windows_logical_disk_read_seconds_total[2m]) and $jp1im_TrendData_labels) + (rate(windows_logical_disk_write_seconds_total[2m]) and $jp1im_TrendData_labels)) / ((rate(windows_logical_disk_reads_total[2m]) and $jp1im_TrendData_labels) + (rate(windows_logical_disk_writes_total[2m]) and $jp1im_TrendData_labels))
resource_en	category	platform_windows
	label	Disk I/O latency
	description	Average time (in seconds) taken to perform a single disk write and read operation
	unit	second
resource_ja	category	platform_windows
	label	ディスク IO レイテンシー
	description	1 回あたりのディスク書き込みと読み込みにかかった平均時間（秒）。
	unit	秒

#

Equivalent to Avg Disk Secs/Xfer field in the PI_LOGD record in JP1/PFM - Agent for Platform (Windows).

- network_sent#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		network_sent
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		rate(windows_net_packets_sent_total[2m]) and $jp1im_TrendData_labels
resource_en	category	platform_windows
	label	Network sent
	description	Rate at which packets were sent through the network interface. [Units: packets/second]

Member name		Configuration contents (default status)
	unit	packets/second
resource_ja	category	platform_windows
	label	ネットワークの送信速度
	description	ネットワークインターフェースで送信されるパケットの割合（パケット／秒）。
	unit	パケット/秒

#

JP1/PFM - Equivalent to the Pkts Sent/sec field in the Agent for Platform (Windows) PI_NETI record.

- network_received#

■Configuration contents (default status)

Member name		Configuration contents (default status)
name		network_received
default		false
promql for metric definition files (including $jp 1im_TrendData_labels)		rate(windows_net_packets_received_total[2m]) and $jp1im_TrendData_labels
resource_en	category	platform_windows
	label	Network received
	description	Rate at which packets were received through the network interface. [Units: packets/second]
	unit	packets/second
resource_ja	category	platform_windows
	label	ネットワークの受信速度
	description	ネットワークインターフェースで受信されるパケットの割合（パケット／秒）。
	unit	パケット/秒

#

JP1/PFM - Equivalent to the Pkts Rcvd/sec field in the Agent for Platform (Windows) PI_NETI record.

Windows exporter (process monitoring) metric definition file (metrics_windows_exporter_process.conf)

Syntax

The same as the JP1/IM - Agent Windows exporter metric definition file.

File

`metrics_windows_exporter_process.conf`

`metrics_windows_exporter_process.conf.model` (Model file)

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines Windows exporter (process monitoring) metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins. If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

The same as the JP1/IM - Agent Windows exporter metric definition file.

Content description

The same as the JP1/IM - Agent Windows exporter metric definition file.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the Windows exporter (process monitoring) metric definition file (model file).

- process_pgm_process_count#
  - Settings (initial status)

Member		Setting (initial status)
name		process_pgm_process_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		count by (instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (windows_process_start_time and $jp1im_TrendData_labels)
resource_en	category	platform_windows_process
	label	Process count
	description	Number of processes that are executing programs. Number of processes that have this program name inside the process table. [Units: count]
	unit	count

#

This has no equivalent field in JP1/PFM - Agent for Platform (Windows). This is equivalent to the PROCESS_COUNT field (addition for alive monitoring) in the JP1/PFM - Agent for Platform (UNIX) PD_PGM record.

Windows exporter (Service monitoring) metric definition file (metrics_windows_exporter_service.conf)

Syntax

See *Syntax* in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_windows_exporter_service.conf`

`metrics_windows_exporter_service.conf.model` (Model file)

Storage directory

- Integration Manager host

For Windows

- When using a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- When using a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

- When using a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- When using a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

Used to get the trend with the service monitoring function of Windows. For details about the service monitor function, see *Specifying monitored services* in *3.15.1(1)(c) Windows exporter (Windows performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This definition file defines metric that can be retrieved by IM management node of the service.

If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the Trends tab on the Integrated Operation Viewer window, or in the REST API.

Content description

See Content description in *Node exporter metric definition file (metrics_node_exporter.conf)*in (2. Definition Files) JP1/IM - Agent.

Settings in the model file (initial status)

The following table shows metric settings (initial status) described in Windows exporter (Service monitoring) metric definition file model file.

- service_state[#]
  - Settings (initial status)

Member		Setting (initial status)
name		service_state
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		windows_service_state{state=\"running\"} and $jp1im_TrendData_labels
resource_en	category	platform_windows_service
	label	Service state
	description	Shows the state of the service. 0: Indicates that the service is not running. 1: Indicates that the service is running
	unit	-

#

Equivalent to State field in the PD_SVC record in JP1/PFM - Agent for Platform (Windows).

Node exporter for AIX metric definition file (metrics_node_exporter_aix.conf)

Syntax

See *Syntax* in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_node_exporter_aix.conf`

`metrics_node_exporter_aix.conf.model` (Model file)

Storage directory

- Integration Manager host

For Windows

- When using a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- When using a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

- When using a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- When using a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines Node exporter for AIX metric information shown in the Trends tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins.

If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the Trends tab on the Integrated Operation Viewer window, or in the REST API.

Content description

See Content description in *Node exporter metric definition file (metrics_node_exporter.conf)* in (2. Definition Files) JP1/IM - Agent.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the Node exporter for AIX metric definition file.

- cpu_used_rate#

  - Settings (initial status)

Member		Setting (initial status)
name		cpu_used_rate
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		((avg by(instance,job,jp1_pc_nodelabel,jp1_pc_prome_hostname) (rate(node_cpu{mode=\"sys\"}[2m]) and $jp1im_TrendData_labels)) +(avg by(instance,job,jp1_pc_nodelabel,jp1_pc_prome_hostname) ((rate(node_cpu{mode=\"user\"}[2m]) and $jp1im_TrendData_labels))))*100
resource_en	category	platform_unix
	label	CPU used rate
	description	CPU usage.It also indicates the average value per processor. [Units: %]
	unit	%

#

Equivalent to CPU% field in the PI record in JP1/PFM - Agent for Platform (UNIX).

See *Precautions When Using SMT or Micro-Partitioning* in *3.15.1(1)(f) Node exporter for AIX (AIX performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- memory_unused#

  - Settings (initial status)

Member		Setting (initial status)
name		memory_unused
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(aix_memory_real_avail and $jp1im_TrendData_labels)/1024/1024/1024*4096
resource_en	category	platform_unix
	label	Memory unused
	description	Size of the physical memory that can actually be used by the application.
	unit	GB

#

Equivalent to "Effective Free Mem Mbytes" field in the PI record in JP1/PFM - Agent for Platform (UNIX), but with different values. For the data sources of Node exporter for AIX, see *Main items to be acquired* in *3.15.1(f) Node exporter for AIX (AIX performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- memory_unused_rate#

  - Settings (initial status)

Member		Setting (initial status)
name		memory_unused_rate
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(aix_memory_real_avail and $jp1im_TrendData_labels)/ (aix_memory_real_total and $jp1im_TrendData_labels) * 100
resource_en	category	platform_unix
	label	Available memory percentage
	description	Percentage of physical memory actually available to the application.
	unit	%

#

Equivalent to "Effective Free Mem %" field in the PI record in JP1/PFM - Agent for Platform (UNIX), but with different values. For the data sources of Node exporter for AIX, see *Main items to be acquired* in *3.15.1(f) Node exporter for AIX (AIX performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- disk_unused#

  - Settings (initial status)

Member		Setting (initial status)
name		disk_unused
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(node_filesystem_free_bytes and $jp1im_TrendData_labels)/(1024*1024*1024)
resource_en	category	platform_unix
	label	Disk unused
	description	Size of the unused area of the disk. [Units: GB]
	unit	GB

#

Equivalent to "Mbytes Free" field in the PD_FSL record in JP1/PFM - Agent for Platform (UNIX).

- disk_unused_rate#

  - Settings (initial status)

Member	Setting (initial status)
name	disk_unused_rate
default	false

Member		Setting (initial status)
promql for the metric definition file (including $jp1im_TrendData_labels)		(node_filesystem_free_bytes and $jp1im_TrendData_labels) / (node_filesystem_size_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	platform_unix
	label	Unused disk space percentage
	description	Percentage of unused disk space.
	unit	%

#

Equivalent to "Mbytes Free %" field in the PD_FSL record in JP1/PFM - Agent for Platform (UNIX).

- disk_busy_rate#

  - Settings (initial status)

Member		Setting (initial status)
name		disk_busy_rate
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(rate(aix_disk_time[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Disk busy rate
	description	Percentage of time the disk was busy with read and write requests. This value may exceed 100 when processe s are continuously executed on a device. [Units: %]
	unit	%

#

Equivalent to "Busy %" field in the PI_DEVD record in JP1/PFM - Agent for Platform (UNIX).

- disk_read_latency#1

  - Settings (initial status)

Member		Setting (initial status)
name		disk_read_latency
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)#2		(rate(aix_disk_rserv[2m]) and $jp1im_TrendData_labels) / (rate(aix_disk_xrate[2m]) and $jp1im_TrendData_labels)/1000/1000/1000
resource_en	category	platform_unix
	label	Disk read latency
	description	Average time (in seconds) taken to perform a single disk read operation.
	unit	second

#1

There are no equivalent fields in JP1/PFM - Agent for Platform (UNIX).

#2

If the value specified in PromQL expression's range vector type (the value specified in square brackets `[ ]`) is not read from the disc, PromQL expression calculates no value.

- disk_write_latency#1

  - Settings (initial status)

Member		Setting (initial status)
name		disk_write_latency
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)#2		(rate(aix_disk_wserv[2m]) and $jp1im_TrendData_labels) / ((rate(aix_disk_xfers[2m]) and $jp1im_TrendData_labels) - (rate(aix_disk_xrate[2m]) and $jp1im_TrendData_labels))/1000/1000/1000
resource_en	category	platform_unix
	label	Disk write latency
	description	Average time (in seconds) taken to perform a single disk write operation.
	unit	second

#1

There are no equivalent fields in JP1/PFM - Agent for Platform (UNIX).

#2

If there is no disc write within the value specified by PromQL expression's range vector type (the value specified in square brackets `[ ]`), PromQL expression calculates no value.

- disk_io_latency#1

  - Settings (initial status)

Member		Setting (initial status)
name		disk_io_latency
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)#2		((rate(aix_disk_rserv[2m]) and $jp1im_TrendData_labels) + (rate(aix_disk_wserv[2m]) and $jp1im_TrendData_labels)) / (rate(aix_disk_xfers[2m]) and $jp1im_TrendData_labels)/1000/1000/1000
resource_en	category	platform_unix
	label	Disk I/O latency
	description	Average time (in seconds) taken to perform a single disk write and read operation.
	unit	second

#1

There are no equivalent fields in JP1/PFM - Agent for Platform (UNIX).

#2

If the value specified by PromQL expression's range vector type (the value specified in square brackets []) is not read from or written to the disc, PromQL expression calculates no value.

- network_sent#

  - Settings (initial status)

Member		Setting (initial status)
name		network_sent
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(rate(aix_netinterface_opackets[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Network sent
	description	Rate of transmitting network interface packets. [Units: packets/second]
	unit	packets/second

#

Equivalent to "Pkts Xmitd/sec" field in the PI_NIND record in JP1/PFM - Agent for Platform (UNIX).

- network_received#

  - Settings (initial status)

Member		Setting (initial status)
name		network_received
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		(rate(aix_netinterface_ipackets[2m]) and $jp1im_TrendData_labels)
resource_en	category	platform_unix
	label	Network received
	description	Rate of receiving network interface packets. [Units: packets/second]
	unit	packets/second

#

Equivalent to "Pkts Rcvd/sec" field in the PI_NIND record in JP1/PFM - Agent for Platform (UNIX).

Blackbox exporter metric definition file (metrics_blackbox_exporter.conf)

Format

```
[
  {
    "name":"trend-data-metric-names",
    "default":default-selection-state
    "promql":"PromQL-statement",
    "resource_en":{
      "category":"metric-category-(English)",
      "label":"metric-display-name-(English)",
      "description":"metric-description-(English)",
      "unit":"metric-unit-(English)"
    },
    "resource_ja":{
      "category":"metric-category-(Japanese)",
      "label":"metric-display-name-(Japanese)",
      "description":"metric-description-(Japanese)",
      "unit":"metric-unit-(Japanese)"
    },
    "module": "module name",
    "drop_legend_labels": ["label name", ...]
  }, ...
]#
```

#

The number of elements that can be described in [] is 1 to 1,000. If an out-of-range number of elements is described, a KAJY24609-E error message is output.

File

`metrics_blackbox_exporter.conf`

`metrics_blackbox_exporter.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines the Blackbox exporter metric information displayed on the Trends tab of the Integrated Operation Viewer window.

The defined contents are used for the return values of __metricListGet method and __timeSeriesDataGet method of the JP1/IM - Agent product plug-in.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This is reflected when metric is acquired on the [Trend] tab of Integrated Operation Viewer window or REST API.

Information that is specified

The following value is setup to `module` membership. For values that setup to other members, see the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

Table 2–96: Value to setup for module members of metric definition File

Member name	Optional	Type	Value to set
module	Yes	string	Set the value of module of the IM management node that returns this metric to a string that matches the forward. This member is optional for Blackbox exporter metrics definition files only. Specify 1~255 characters except control characters (0x00~0x1F, 0x7F~0x9F). If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. If omitted, this metric is returned for all remote agent SIDs of the Blackbox exporter. The IM management node's module value is the value specified for module in the Prometheus configuration file (jpc_prometheus_server.yml) scrape job. This value is also displayed in the Module property of the Blackbox exporter's Remote Agent SID. Example 1: http Example 2: ICMP

Model file settings (initial state) and alert definition example

The setting contents (initial state) and alert definition example (alert setting file) of each metric described in the model file of the Blackbox exporter metric definition file are shown below.

- probe_success

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		probe_success
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		probe_success and $jp1im_TrendData_labels
resource_en	category	probe
	label	Probe success or failure
	description	Displays whether or not the probe was a success
	unit	-
resource_ja	category	probe
	label	プローブ成否
	description	プローブが成功したかどうかを表示します。 0：失敗 1：成功
	unit	-
module		Do not specify

- probe_duration_seconds

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		probe_duration_seconds
default		true
The promql for metric definition File (including $jp1im_TrendData_labels)		probe_duration_seconds and $jp1im_TrendData_labels
resource_en	category	probe
	label	Probe period
	description	Returns how long the probe took to complete in seconds
	unit	second
resource_ja	category	probe
	label	プローブ期間
	description	プローブが完了するまでに要した時間を秒単位で返します。
	unit	秒
module		Do not specify

- probe_icmp_duration_seconds

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		probe_icmp_duration_seconds
default		true

Member name		Configuration contents (default status)
The promql for metric definition File (including $jp1im_TrendData_labels)		probe_icmp_duration_seconds and $jp1im_TrendData_labels
resource_en	category	probe
	label	ICMP period
	description	Duration of icmp request
	unit	second
resource_ja	category	probe
	label	ICMP 期間
	description	フェーズごとの ICMP 要求の期間
	unit	秒
module		icmp

- probe_http_duration_seconds

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		probe_http_duration_seconds
default		true
The promql for metric definition File (including $jp1im_TrendData_labels)		probe_http_duration_seconds and $jp1im_TrendData_labels
resource_en	category	probe
	label	HTTP request period
	description	Duration of http request by phase, summed over all redirects
	unit	second
resource_ja	category	probe
	label	HTTP リクエスト期間
	description	フェーズごとの HTTP リクエストの期間，すべてのリダイレクトで合計
	unit	秒
module		http

- probe_http_status_code

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		probe_http_status_code
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		probe_http_status_code and $jp1im_TrendData_labels
resource_en	category	probe
	label	HTTP status

Member name		Configuration contents (default status)
	description	Response HTTP status code
	unit	-
resource_ja	category	probe
	label	HTTP ステータス
	description	HTTP レスポンスステータスコード
	unit	-
module		http

Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf)

Format

```
[
  {
    "name":"trend-data-metric-names",
    "default":default-selection-state,
    "promql":"PromQL-statement",
    "resource_en":{
      "category":"metric-category-(English)",
      "label":"metric-display-name-(English)",
      "description":"metric-description-(English)",
      "unit":"metric-unit-(English)"
    },
    "resource_ja":{
      "category":"metric-category-(Japanese)",
      "label":"metric-display-name-(Japanese)",
      "description":"metric-description-(Japanese)",
      "unit":"metric-unit-(Japanese)"
    },
    "cloud_srv": "AWS service namespace name",
    "drop_legend_labels": ["label-name", ...]
  }, ...
]#
```

#

The number of elements that can be described in [] is 1 to 1,000. If an out-of-range number of elements is described, a KAJY24609-E error message is output.

File

`metrics_ya_cloudwatch_exporter.conf`

`metrics_ya_cloudwatch_exporter.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines the metrics information for Yet another cloudwatch exporter displayed on the Trends tab of the Unified Operations Viewer screen.

The defined contents are used for the return values of __metricListGet method and __timeSeriesDataGet method of the JP1/IM - Agent product plug-in.

IM management nodes for Yet another cloudwatch exporter are created only for resources for metrics defined in the Yet another cloudwatch exporter metrics definition file.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

It is reflected when metric information is obtained on the Trends tab of the [Integrated Operation Viewer] screen or with the REST API.

IM management nodes in Yet another cloudwatch exporter are reflected when you run the jddcreatetree and jddupdatetree commands.

Information that is specified

The following value is setup to `name` and `cloud_srv` membership. For values that setup to other members, see the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

Table 2–97: Values to set for the name and cloud_srv members of the metric definition file

Member name	Optional	Type	Value to set
name	No	string	Set the metric name for the trend data. The metric name of trend data (time series data) is displayed as a character string indicating the type of trend data on the Trend tab of the Unified Operation Viewer screen. For yet another cloudwatch exporter metrics definition file, create only resources for the metrics defined here. Also, the metric name must match the metric name in Yet another cloudwatch exporter. 1 to 255 characters, and the following characters can be specified. • Single-byte alphanumeric characters • - (hyphen) • _ (underscore) If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed. The metric name must be unique within the metric definition file. Otherwise, a KAJY24608-E error message is output.

Member name	Optional	Type	Value to set
cloud_srv	Yes	string	Set the AWS service namespace name. This member is required only for Yet another cloudwatch exporter metrics definition file. Set the name of the following namespace specified in the Yet another cloudwatch exporter configuration file (jpc_ya_cloudwatch_exporter.yml): • Namespace specified by [Auto-discovery job] type# Example 1: AWS/EC2 Example 2: AWS/S33 1 to 255 characters, and the following characters can be specified. • Single-byte alphanumeric characters • . (period) • - (hyphen) • _ (underscore) • / (forward slash) • # (hash) • : (colon) If it contains characters that cannot be specified, a KAJY24604-E or KAJY24605-E error message is printed.

#

For information about the namespaces (services) that can be specified in Auto-discovery job's type, see the section describing the namespaces of AWS that JP1/IM - Agent supports as monitored at *3.15.6(1)(k) Creating an IM management Node for Yet another cloudwatch exporter* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Model file settings (initial state)

The setting contents (initial state) of each metric described in the model file of the Yet another cloudwatch exporter metric definition file are shown below.

- aws_ec2_cpuutilization_average

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_ec2_cpuutilization_average
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_ec2_cpuutilization_average and $jp1im_TrendData_labels
resource_en	category	aws_ec2
	label	CPU utilization
	description	The percentage of the allocated EC2 compute units that are currently in use on the instance. For details, see the description of the CPUUtilization metric for AWS/EC2.
	unit	%
resource_ja	category	aws_ec2
	label	CPU 使用率
	description	割り当てられた EC2 コンピュートユニットのうち，現在インスタンス上で使用されているものの比率。 詳細は AWS/EC2 の CPUUtilization メトリックの説明を参照してください。

Member name		Configuration contents (default status)
	unit	%
cloud_srv		AWS/EC2

- aws_ec2_disk_read_bytes_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_ec2_disk_read_bytes_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(aws_ec2_disk_read_bytes_sum and $jp1im_TrendData_labels) / 1024
resource_en	category	aws_ec2
	label	Amount of data read in KB
	description	Amount of data in KB read from all instance store volumes available to the instance. For more information, see the description of the DiskReadBytes metric of AWS EC2.
	unit	KB
resource_ja	category	aws_ec2
	label	読み取りキロバイト数
	description	インスタンスで利用できるすべてのインスタンスストアボリュームから読み取られたキロバイト数。 詳細は AWS/EC2 の DiskReadBytes メトリックの説明を参照してください。
	unit	キロバイト
cloud_srv		AWS/EC2

- aws_ec2_disk_write_bytes_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_ec2_disk_write_bytes_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(aws_ec2_disk_write_bytes_sum and $jp1im_TrendData_labels) / 1024
resource_en	category	aws_ec2
	label	Amount of data written in KB
	description	Amount of data in KB written to all instance store volumes available to the instance. For more information, see the description of the DiskWriteBytes metric of AWS EC2.
	unit	KB
resource_ja	category	aws_ec2
	label	書き込みキロバイト数
	description	インスタンスで利用できるすべてのインスタンスストアボリュームに書き込まれたキロバイト数。 詳細は AWS/EC2 の DiskWriteBytes メトリックの説明を参照してください。

Member name		Configuration contents (default status)
	unit	キロバイト
cloud_srv		AWS/EC2

- aws_lambda_errors_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_lambda_errors_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_lambda_errors_sum and $jp1im_TrendData_labels
resource_en	category	aws_lambda
	label	Number of invocations
	description	The number of invocations that result in a function error. For details, see the description of the Errors metric for AWS/Lambda.
	unit	count
resource_ja	category	aws_lambda
	label	呼び出し数
	description	関数エラーが発生した呼び出しの数。 詳細は AWS/Lambda の Errors メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/Lambda

- aws_lambda_duration_average

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_lambda_duration_average
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_lambda_duration_average and $jp1im_TrendData_labels
resource_en	category	aws_lambda
	label	Event processing time
	description	The amount of time that your function code spends processing an event. For details, see the description of the Duration metric for AWS/Lambda.
	unit	msec
resource_ja	category	aws_lambda
	label	イベント処理時間
	description	関数コードがイベントの処理に費やす時間。 詳細は AWS/Lambda の Duration メトリックの説明を参照してください。
	unit	ミリ秒

Member name	Configuration contents (default status)
cloud_srv	AWS/Lambda

- aws_s3_bucket_size_bytes_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_s3_bucket_size_bytes_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		(aws_s3_bucket_size_bytes_sum and $jp1im_TrendData_labels) / (1024*1024*1024)
resource_en	category	aws_s3
	label	Amount of data stored
	description	The amount of data in GB stored in a bucket in the STANDARD storage class, INTELLIGENT_TIERING storage class, Standard-Infrequent Access (STANDARD_IA) storage class, OneZone-Infrequent Access (ONEZONE_IA), Reduced Redundancy Storage (RRS) class, Deep Archive Storage (S3 Glacier Deep Archive) class or, Glacier (GLACIER) storage class. For details, see the description of the BucketSizeBytes metric for AWS/S3.
	unit	GB
resource_ja	category	aws_s3
	label	保存データ量
	description	STANDARDストレージクラス，INTELLIGENT_TIERINGストレージクラス，標準低頻度アクセス（STANDARD_IA）ストレージクラス，OneZone低頻度アクセス（ONEZONE_IA），低冗長化ストレージ(RRS)クラス，ディープアーカイブストレージ（S3 Glacier Deep Archive），またはGlacier（GLACIER）ストレージクラスのバケットに保存されているデータの量（ギガバイト単位）。 詳細はAWS/S3のBucketSizeBytesメトリックの説明を参照してください。
	unit	ギガバイト
cloud_srv		AWS/S3

- aws_s3_5xx_errors_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_s3_5xx_errors_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_s3_5xx_errors_sum and $jp1im_TrendData_labels
resource_en	category	aws_s3
	label	Number of 5xx server errors
	description	The number of HTTP 5xx server error status code requests made to an Amazon S3 bucket with a value of either 0 or 1. For details, see the description of the 5xx_errors metric for AWS/S3.
	unit	count
resource_ja	category	aws_s3

Member name		Configuration contents (default status)
	label	5xx サーバエラー数
	description	Amazon S3 バケットに対して行われた，値が 0 または 1 の HTTP 5xx サーバーエラーステータスコードリクエストの数。 詳細は AWS/S3 の 5xx_errors メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/S3

- aws_dynamodb_consumed_read_capacity_units_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_dynamodb_consumed_read_capacity_units_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_dynamodb_consumed_read_capacity_units_sum and $jp1im_TrendData_labels
resource_en	category	aws_dynamo_db
	label	Number of read capacity units
	description	The total number of read capacity units consumed. For details, see the description of the ConsumedReadCapacityUnits metric for Amazon DynamoDB.
	unit	count
resource_ja	category	aws_dynamo_db
	label	読み込み容量ユニット数
	description	消費された読み込み容量ユニットの合計。 詳細は Amazon DynamoDB の ConsumedReadCapacityUnits メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/DynamoDB

- aws_dynamodb_consumed_write_capacity_units_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_dynamodb_consumed_write_capacity_units_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_dynamodb_consumed_write_capacity_units_sum and $jp1im_TrendData_labels
resource_en	category	aws_dynamo_db
	label	Number of write capacity units
	description	The total number of write capacity units consumed. For details, see the description of the ConsumedWriteCapacityUnits metric for Amazon DynamoDB.
	unit	count
resource_ja	category	aws_dynamo_db

Member name		Configuration contents (default status)
	label	書き込み容量ユニット数
	description	消費された書き込み容量ユニットの合計。 詳細は Amazon DynamoDB の ConsumedWriteCapacityUnits メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/DynamoDB

- aws_states_execution_time_average

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_states_execution_time_average
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_states_execution_time_average and $jp1im_TrendData_labels
resource_en	category	aws_states
	label	Execution time
	description	The average of the interval, in milliseconds, from the start to the end of the execution of Step Functions. For details, see the description of the ExecutionTime metric for AWS Step Functions.
	unit	msec
resource_ja	category	aws_states
	label	実行時間
	description	Step Functions の実行の開始時点から終了時点までの間隔の平均値（ミリ秒単位）。 詳細は AWS Step Functions の ExecutionTime メトリックの説明を参照してください。
	unit	ミリ秒
cloud_srv		AWS/States

- aws_states_executions_failed_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_states_executions_failed_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_states_executions_failed_sum and $jp1im_TrendData_labels
resource_en	category	aws_states
	label	Number of failed executions
	description	The total number of failed executions of Step Functions. For details, see the description of the ExecutionsFailed metric for AWS Step Functions.
	unit	count

Member name		Configuration contents (default status)
resource_ja	category	aws_states
	label	実行失敗数
	description	Step Functions の失敗した実行の合計数。 詳細は AWS Step Functions の ExecutionsFailed メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/States

- aws_sqs_approximate_number_of_messages_delayed_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_sqs_approximate_number_of_messages_delayed_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_sqs_approximate_number_of_messages_delayed_sum and $jp1im_TrendData_labels
resource_en	category	aws_sqs
	label	Number of messages in the delay queue
	description	The total number of messages in the queue that are delayed and not available for reading immediately. For details, see the description of the ApproximateNumberOfMessagesDelayed metric for Amazon SQS.
	unit	count
resource_ja	category	aws_sqs
	label	遅延キューメッセージ数
	description	遅延が発生したため，すぐに読み取ることのできない，キューのメッセージの合計数。 詳細は Amazon SQS の ApproximateNumberOfMessagesDelayed メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/SQS

- aws_sqs_number_of_messages_deleted_sum

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		aws_sqs_number_of_messages_deleted_sum
default		false
The promql for metric definition File (including $jp1im_TrendData_labels)		aws_sqs_number_of_messages_deleted_sum and $jp1im_TrendData_labels
resource_en	category	aws_sqs
	label	Number of messages in the deletion queue
	description	The total number of messages deleted from the queue. For details, see the description of the NumberOfMessagesDeleted metric for Amazon SQS.

Member name		Configuration contents (default status)
	unit	count
resource_ja	category	aws_sqs
	label	削除キューメッセージ数
	description	キューから削除されたメッセージの合計数。 詳細は Amazon SQS の NumberOfMessagesDeleted メトリックの説明を参照してください。
	unit	個
cloud_srv		AWS/SQS

- aws_ebs_volume_read_bytes_sum
  - Settings (initial status)

Member		Setting (initial status)
name		aws_ebs_volume_read_bytes_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_ebs_volume_read_bytes_sum and $jp1im_TrendData_labels
resource_en	category	aws_ebs
	label	Number of bytes read
	description	Total number of bytes transferred in read operations over the specified time period. For details, see the description of the VolumeReadBytes metric for AWS/EBS.
	unit	byte
cloud_srv		AWS/EBS

- aws_ebs_volume_write_bytes_sum
  - Settings (initial status)

Member		Setting (initial status)
name		aws_ebs_volume_write_bytes_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_ebs_volume_write_bytes_sum and $jp1im_TrendData_labels
resource_en	category	aws_ebs
	label	Number of bytes written
	description	Total number of bytes transferred in write operations over the specified time period. For details, see the description of the VolumeWriteBytes metric for AWS/EBS.
	unit	byte
cloud_srv		AWS/EBS

- aws_ecs_cpuutilization_average
  - Settings (initial status)

Member		Setting (initial status)
name		aws_ecs_cpuutilization_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_ecs_cpuutilization_average and $jp1im_TrendData_labels
resource_en	category	aws_ecs
	label	CPU utilization
	description	Percentage of CPU used by the cluster or service. For details, see the description of the CPUUtilization metric for AWS/ECS.
	unit	%
cloud_srv		AWS/ECS

- aws_ecs_memory_utilization_average
  - Settings (initial status)

Member		Setting (initial status)
name		aws_ecs_memory_utilization_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_ecs_memory_utilization_average and $jp1im_TrendData_labels
resource_en	category	aws_ecs
	label	Memory utilization
	description	Percentage of memory utilized by the cluster or service. For details, see the description of the MemoryUtilization metric for AWS/ECS.
	unit	%
cloud_srv		AWS/ECS

- aws_efs_total_iobytes_average
  - Settings (initial status)

Member		Setting (initial status)
name		aws_efs_total_iobytes_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_efs_total_iobytes_average and $jp1im_TrendData_labels
resource_en	category	aws_efs
	label	Total bytes
	description	The actual number of bytes for each file system operation, including read data, write data, and metadata operations. For details, see the description of the TotalIOBytes metric for AWS/EFS.
	unit	byte
cloud_srv		AWS/EFS

- aws_efs_storage_bytes_average

- Settings (initial status)

Member		Setting (initial status)
name		aws_efs_storage_bytes_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_efs_storage_bytes_average and $jp1im_TrendData_labels
resource_en	category	aws_efs
	label	Storage usage
	description	File system size in bytes. For details, see the description of the StorageBytes metric for AWS/EFS.
	unit	byte
cloud_srv		AWS/EFS

- aws_fsx_data_read_bytes_sum
  - Settings (initial status)

Member		Setting (initial status)
name		aws_fsx_data_read_bytes_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_fsx_data_read_bytes_sum and $jp1im_TrendData_labels
resource_en	category	ws_fsx
	label	Number of bytes read
	description	Number of bytes in file system read operations. For details, see the description of the DataReadBytes metric for AWS/FSx.
	unit	byte
cloud_srv		AWS/FSx

- aws_fsx_data_write_bytes_sum
  - Settings (initial status)

Member		Setting (initial status)
name		aws_fsx_data_write_bytes_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_fsx_data_write_bytes_sum and $jp1im_TrendData_labels
resource_en	category	aws_fsx
	label	Number of bytes written
	description	Number of bytes in file system write operations. For details, see the description of the DataWriteBytes metric for AWS/FSx.
	unit	byte
cloud_srv		AWS/FSx

- aws_fsx_free_storage_capacity_average

- Settings (initial status)

Member		Setting (initial status)
name		aws_fsx_free_storage_capacity_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_fsx_free_storage_capacity_average and $jp1im_TrendData_labels
resource_en	category	aws_fsx
	label	Free space
	description	Available storage capacity. For details, see the description of the FreeStorageCapacity metric for AWS/FSx.
	unit	byte
cloud_srv		AWS/FSx

- aws_rds_cpuutilization_average
  - Settings (initial status)

Member		Setting (initial status)
name		aws_rds_cpuutilization_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_rds_cpuutilization_average and $jp1im_TrendData_labels
resource_en	category	aws_rds
	label	CPU utilization
	description	CPU utilization. For details, see the description of the CPUUtilization metric for AWS/RDS.
	unit	%
cloud_srv		AWS/RDS

- aws_rds_read_iops_average
  - Settings (initial status)

Member		Setting (initial status)
name		aws_rds_read_iops_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_rds_read_iops_average and $jp1im_TrendData_labels
resource_en	category	aws_rds
	label	Read IOPS
	description	Average number of disk read I/O operations per second. For details, see the description of the ReadIOPS metric for AWS/RDS.
	unit	count/second
cloud_srv		AWS/RDS

- aws_rds_write_iops_average

- Settings (initial status)

Member		Setting (initial status)
name		aws_rds_write_iops_average
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_rds_write_iops_average and $jp1im_TrendData_labels
resource_en	category	aws_rds
	label	Write IOPS
	description	Average number of disk write I/O operations per second. For details, see the description of the WriteIOPS metric for AWS/RDS.
	unit	count/second
cloud_srv		AWS/RDS

- aws_sns_number_of_notifications_failed_sum

  - Settings (initial status)

Member		Setting (initial status)
name		aws_sns_number_of_notifications_failed_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_sns_number_of_notifications_failed_sum and $jp1im_TrendData_labels
resource_en	category	aws_sns
	label	Number of failed notifications
	description	The number of messages that Amazon SNS failed to deliver. For details, see the description of the NumberOfNotificationsFailed metric for AWS/SNS.
	unit	count
cloud_srv		AWS/SNS

- aws_sns_number_of_notifications_filtered_out_sum

  - Settings (initial status)

Member		Setting (initial status)
name		aws_sns_number_of_notifications_filtered_out_sum
default		FALSE
promql for the metric definition file (including $jp1im_TrendData_labels)		aws_sns_number_of_notifications_filtered_out_sum and $jp1im_TrendData_labels
resource_en	category	aws_sns
	label	Number of filterd out notifications
	description	Number of messages rejected by subscription filter policy. For details, see the description of the NumberOfNotificationsFilteredOut metric for AWS/SNS.
	unit	count
cloud_srv		AWS/SNS

Promitor metric definition file (metrics_promitor.conf)

Syntax

The same as the JP1/IM - Agent Node exporter metric definition file.

File

`metrics_promitor.conf`

`metrics_promitor.conf.model` (Model file)

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs_azure\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs_azure\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs_azure/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs_azure/`

Description

This file defines Promitor metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins.

The Promitor IM management node is only created for metric resources defined in the Promitor metric definition file. If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the **Trends** tab on the Integrated Operation Viewer window, or in the REST API.

For the Promitor IM management node, definitions are reflected when the jddcreatetree command and the jddupdatetree command are executed.

Content description

The same as the JP1/IM - Agent Node exporter metric definition file.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the Promitor metric definition file (model file).

- azure_virtual_machine_disk_read_bytes_total
  - Settings (initial status)

Member		Setting (initial status)
name		azure_virtual_machine_disk_read_bytes_total
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_virtual_machine_disk_read_bytes_total and $jp1im_TrendData_labels
resource_en	category	azure_virtual_machine
	label	Disk read bytes
	description	Bytes read from disk during monitoring period. For details, see the description of the Disk Read Bytes metric for Microsoft.Compute/virtualMachines.
	unit	byte
cloud_srv		Azure/VirtualMachine

- azure_virtual_machine_disk_write_bytes_total
  - Settings (initial status)

Member		Setting (initial status)
name		azure_virtual_machine_disk_write_bytes_total
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_virtual_machine_disk_write_bytes_total and $jp1im_TrendData_labels
resource_en	category	azure_virtual_machine
	label	Disk write bytes
	description	Bytes written to disk during monitoring period. For details, see the description of the Disk Write Bytes metric for Microsoft.Compute/virtualMachines.
	unit	byte
cloud_srv		Azure/VirtualMachine

- azure_virtual_machine_percentage_cpu_average
  - Settings (initial status)

Member	Setting (initial status)
name	azure_virtual_machine_percentage_cpu_average
default	false

Member		Setting (initial status)
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_virtual_machine_percentage_cpu_average and $jp1im_TrendData_labels
resource_en	category	azure_virtual_machine
	label	Percentage of allocated compute units
	description	The percentage of allocated compute units that are currently in use by the Virtual Machine(s). For details, see the description of the Percentage CPU metric for Microsoft.Compute/virtualMachines.
	unit	%
cloud_srv		Azure/VirtualMachine

- azure_blob_storage_availability_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_blob_storage_availability_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_blob_storage_availability_average and $jp1im_TrendData_labels
resource_en	category	azure_blob_storage
	label	Percentage of availability
	description	The percentage of availability for the storage service or the specified API operation. For details, see the description of the Availability metric for Microsoft.Storage/storageAccounts/blobServices.
	unit	%
cloud_srv		Azure/BlobStorage

- azure_blob_storage_blob_capacity_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_blob_storage_blob_capacity_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_blob_storage_blob_capacity_average and $jp1im_TrendData_labels
resource_en	category	azure_blob_storage
	label	Amount of storage
	description	The amount of storage used by the storage account's Blob service in bytes. For details, see the description of the BlobCapacity metric for Microsoft.Storage/storageAccounts/blobServices.
	unit	byte
cloud_srv		Azure/BlobStorage

- azure_function_app_http5xx_total
  - Settings (initial status)

Member		Setting (initial status)
name		azure_function_app_http5xx_total
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_function_app_http5xx_total and $jp1im_TrendData_labels
resource_en	category	azure_function_app
	label	Number of 5xx server errors
	description	The count of requests resulting in an HTTP status code >= 500 but < 600. For details, see the description of the Http5xx metric for Microsoft.Web/sites.
	unit	count
cloud_srv		Azure/FunctionApp

- azure_function_app_http_response_time_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_function_app_http_response_time_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_function_app_http_response_time_average and $jp1im_TrendData_labels
resource_en	category	azure_function_app
	label	Response time
	description	The time taken for the app to serve requests, in seconds. For details, see the description of the HttpResponseTime metric for Microsoft.Web/sites.
	unit	sec
cloud_srv		Azure/FunctionApp

- azure_cosmos_db_total_request_units_total
  - Settings (initial status)

Member		Setting (initial status)
name		azure_cosmos_db_total_request_units_total
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_cosmos_db_total_request_units_total and $jp1im_TrendData_labels
resource_en	category	azure_cosmos_db
	label	Request Units consumed
	description	Request Units consumed. For details, see the description of the TotalRequestUnits metric for Microsoft.DocumentDB/DatabaseAccounts.
	unit	count
cloud_srv		Azure/CosmosDb

- azure_logic_app_runs_failed_total
  - Settings (initial status)

Member		Setting (initial status)
name		azure_logic_app_runs_failed_total
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_logic_app_runs_failed_total and $jp1im_TrendData_labels
resource_en	category	azure_logic_app
	label	Number of workflow runs failed
	description	Number of workflow runs failed. For details, see the description of the RunsFailed metric for Microsoft.Logic/Workflows.
	unit	count
cloud_srv		Azure/LogicApp

- azure_container_instance_cpu_usage_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_container_instance_cpu_usage_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_container_instance_cpu_usage_average and $jp1im_TrendData_labels
resource_en	category	azure_container_instance
	label	CPU usage
	description	CPU usage on all cores in millicores. For details, see the description of the CpuUsage metric for Microsoft.ContainerInstance/containerGroups.
	unit	count
cloud_srv		Azure/ContainerInstance

- azure_container_instance_memory_usage_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_container_instance_memory_usage_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_container_instance_memory_usage_average and $jp1im_TrendData_labels
resource_en	category	azure_container_instance
	label	Total memory usage
	description	Total memory usage in byte. For details, see the description of the MemoryUsage metric for Microsoft.ContainerInstance/containerGroups.
	unit	byte
cloud_srv		Azure/ContainerInstance

- azure_kubernetes_service_kube_pod_status_phase_average_failed
  - Settings (initial status)

Member		Setting (initial status)
name		azure_kubernetes_service_kube_pod_status_phase_average_failed
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_kubernetes_service_kube_pod_status_phase_average_failed and $jp1im_TrendData_labels
resource_en	category	azure_kubernetes_service
	label	Number of failed pods
	description	Number of failed pods. For details, see the description of the kube_pod_status_phase metric for Microsoft.ContainerService/managedClusters.
	unit	count
cloud_srv		Azure/KubernetesService

- azure_kubernetes_service_kube_pod_status_phase_average_pending
  - Settings (initial status)

Member		Setting (initial status)
name		azure_kubernetes_service_kube_pod_status_phase_average_pending
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_kubernetes_service_kube_pod_status_phase_average_pending and $jp1im_TrendData_labels
resource_en	category	azure_kubernetes_service
	label	Number of pending pods
	description	Number of pending pods. For details, see the description of the kube_pod_status_phase metric for Microsoft.ContainerService/managedClusters.
	unit	count
cloud_srv		Azure/KubernetesService

- azure_kubernetes_service_kube_pod_status_phase_average_unknown
  - Settings (initial status)

Member		Setting (initial status)
name		azure_kubernetes_service_kube_pod_status_phase_average_unknown
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_kubernetes_service_kube_pod_status_phase_average_unknown and $jp1im_TrendData_labels
resource_en	category	azure_kubernetes_service
	label	Number of unknown pods
	description	Number of unknown pods. For details, see the description of the kube_pod_status_phase metric for Microsoft.ContainerService/managedClusters.
	unit	count
cloud_srv		Azure/KubernetesService

- azure_file_storage_availability_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_file_storage_availability_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_file_storage_availability_average and $jp1im_TrendData_labels
resource_en	category	azure_file_storage
	label	Percentage of availability
	description	The percentage of availability for the storage service or the specified API operation. For details, see the description of the Availability metric for Microsoft.Storage/storageAccounts/fileServices.
	unit	%
cloud_srv		Azure/FileStorage

- azure_file_storage_file_capacity_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_file_storage_file_capacity_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_file_storage_file_capacity_average and $jp1im_TrendData_labels
resource_en	category	azure_file_storage
	label	Amount of file storage
	description	The amount of File storage used by the storage account. For details, see the description of the FileCapacity metric for Microsoft.Storage/storageAccounts/fileServices.
	unit	byte
cloud_srv		Azure/FileStorage

- azure_service_bus_namespace_deadlettered_messages_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_service_bus_namespace_deadlettered_messages_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_service_bus_namespace_deadlettered_messages_average and $jp1im_TrendData_labels
resource_en	category	azure_service_bus_namespace
	label	Number of dead-lettered messages
	description	Count of dead-lettered messages in a Queue/Topic. For details, see the description of the DeadletteredMessages metric for Microsoft.ServiceBus/Namespaces.
	unit	count
cloud_srv		Azure/ServiceBusNamespace

- azure_sql_database_cpu_percent_average

- Settings (initial status)

Member		Setting (initial status)
name		azure_sql_database_cpu_percent_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_database_cpu_percent_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_database
	label	CPU percentage
	description	CPU percentage. For details, see the description of the cpu_percent metric for Microsoft.Sql/servers/databases.
	unit	%
cloud_srv		Azure/SqlDatabase

- azure_sql_database_dtu_used_average

  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_database_dtu_used_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_database_dtu_used_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_database
	label	DTU used
	description	DTU used. For details, see the description of the dtu_used metric for Microsoft.Sql/servers/databases.
	unit	count
cloud_srv		Azure/SqlDatabase

- azure_sql_database_storage_maximum

  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_database_storage_maximum
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_database_storage_maximum and $jp1im_TrendData_labels
resource_en	category	azure_sql_database
	label	Data space used
	description	Data space used. For details, see the description of the storage metric for Microsoft.Sql/servers/databases.
	unit	byte
cloud_srv		Azure/SqlDatabase

- azure_sql_elastic_pool_cpu_percent_average

- Settings (initial status)

Member		Setting (initial status)
name		azure_sql_elastic_pool_cpu_percent_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_elastic_pool_cpu_percent_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_elastic_pool
	label	CPU percentage
	description	CPU percentage. For details, see the description of the cpu_percent metric for Microsoft.Sql/servers/elasticpools.
	unit	%
cloud_srv		Azure/SqlElasticPool

- azure_sql_elastic_pool_e_dtu_used_average

  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_elastic_pool_e_dtu_used_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_elastic_pool_e_dtu_used_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_elastic_pool
	label	eDTU used
	description	eDTU used. For details, see the description of the eDTU_used metric for Microsoft.Sql/servers/elasticpools.
	unit	count
cloud_srv		Azure/SqlElasticPool

- azure_sql_elastic_pool_storage_used_average

  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_elastic_pool_storage_used_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_elastic_pool_storage_used_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_elastic_pool
	label	Data space used
	description	Data space used. For details, see the description of the storage_used metric for Microsoft.Sql/servers/elastipools.
	unit	byte
cloud_srv		Azure/SqlElasticPool

- azure_sql_managed_instance_avg_cpu_percent_average

- Settings (initial status)

Member		Setting (initial status)
name		azure_sql_managed_instance_avg_cpu_percent_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_managed_instance_avg_cpu_percent_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_managed_instance
	label	Average CPU percentage
	description	Average CPU percentage. For details, see the description of the avg_cpu_percent metric for Microsoft.Sql/managedInstances.
	unit	%
cloud_srv		Azure/SqlManagedInstance

- azure_sql_managed_instance_io_bytes_read_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_managed_instance_io_bytes_read_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_managed_instance_io_bytes_read_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_managed_instance
	label	IO bytes read
	description	IO bytes read. For details, see the description of the io_bytes_read metric for Microsoft.Sql/managedInstances.
	unit	byte
cloud_srv		Azure/SqlManagedInstance

- azure_sql_managed_instance_io_bytes_written_average
  - Settings (initial status)

Member		Setting (initial status)
name		azure_sql_managed_instance_io_bytes_written_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_managed_instance_io_bytes_written_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_managed_instance
	label	IO bytes written
	description	IO bytes written. For details, see the description of the io_bytes_written metric for Microsoft.Sql/managedInstances.
	unit	byte
cloud_srv		Azure/SqlManagedInstance

- azure_sql_managed_instance_storage_space_used_mb_average

- Settings (initial status)

Member		Setting (initial status)
name		azure_sql_managed_instance_storage_space_used_mb_average
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		azure_sql_managed_instance_storage_space_used_mb_average and $jp1im_TrendData_labels
resource_en	category	azure_sql_managed_instance
	label	Storage space used
	description	Storage space used. For details, see the description of the storage_space_used_mb metric for Microsoft.Sql/managedInstances.
	unit	count
cloud_srv		Azure/SqlManagedInstance

Script exporter metric definition file (metrics_script_exporter.conf)

Syntax

The same as the JP1/IM - Agent Node exporter metric definition file.

File

`metrics_script_exporter.conf`

`metrics_script_exporter.conf.model` (Model file)

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines Script exporter metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins. If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the **Trends** tab on the Integrated Operation Viewer window, or in the REST API.

For the Script exporter IM management node, definitions are reflected when the jddcreatetree command and the jddupdatetree command are executed.

Content description

See *Content description* in *Node exporter metric definition file (metrics_node_exporter.conf)* in *(2. Definition Files)* JP1/IM - Agent.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the Script exporter metric definition file (model file).

- azure_virtual_machine_disk_read_bytes_total
  - Settings (initial status)

Member		Setting (initial status)
name		script_success
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		script_success and $jp1im_TrendData_labels
resource_en	category	script
	label	Script success
	description	Script exit status (0 = error, 1 = success)
	unit	-

- script_duration_seconds
  - Settings (initial status)

Member		Setting (initial status)
name		script_duration_seconds
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		script_duration_seconds and $jp1im_TrendData_labels
resource_en	category	script
	label	Duration
	description	Script execution time, in seconds
	unit	seconds

- script_exit_code
  - Settings (initial status)

Member		Setting (initial status)
name		script_exit_code
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		script_exit_code and $jp1im_TrendData_labels
resource_en	category	script
	label	Exit code

Member		Setting (initial status)
	description	Script execution time, in seconds
	unit	-

Fluentd metric definition file (metrics_fluentd.conf)

Format

See the *Format* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_fluentd.conf`

`metrics_fluentd.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This File defines metric of Fluentd to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.

Defined content is used for the __metricListGet method of product plugin in JP1/IM - Agent and the return Value of the __timeSeriesDataGet method.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This is reflected when metric is acquired on the [Trend] tab of Integrated Operation Viewer window or REST API.

Information that is specified

See the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

Model File's Configuration contents (Default status)

Configuration contents (default status) of metric described in file of Fluentd metric definition file is shown below.

- fluentd_logtrap_running

  ■Configuration contents (default status)

Member name		Configuration contents (default status)
name		fluentd_logtrap_running
default		true
The promql for metric definition File (including $jp1im_TrendData_labels)		fluentd_logtrap_running and $jp1im_TrendData_labels
resource_en	category	fluentd_logtrap
	label	Log monitoring status
	description	The value is always 1 and indicates that the log is being monitored. If the sample is not displayed, no log monitoring has been performed for that time. 1: monitoring is being done
	unit	-
resource_ja	category	fluentd_logtrap
	label	ログ監視状況
	description	値は常に 1 で，ログの監視が行われていることを表します。サンプルが表示されない場合，その時間のログ監視は行われていません。 1：監視が行われている
	unit	-

OracleDB exporter metric definition file (metrics_oracledb_exporter.conf)

Syntax

See *Syntax* in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_oracledb_exporter.conf`

`metrics_oracledb_exporter.conf.model (model file)`

Storage directory

- Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This file defines OracleDB exporter metric information shown in the Trends tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins.

If JP1/IM - Manager is in a hierarchical configuration and you want the integrated manager to refer to trend data stored in trend data management database of lower manager, you must add the referenced trend data metrics to the integrated manager metric definition file.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the Trends tab on the Integrated Operation Viewer window, or in the REST API.

Content description

See *Content description* in *Node exporter metric definition file (metrics_node_exporter.conf)* in (2. Definition Files) JP1/IM - Agent.

Model file settings (initial state)

The following shows the settings (initial status) of each metric written in the OracleDB exporter metric definition file.

- oracledb_up

  - Settings (initial status)

Member		Setting (initial status)
name		oracledb_up
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		oracledb_up and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	OracleDB Startup Status
	description	Shows the startup status of OracleDB. 1 indicates that it is running, while 0 indicates that it is stopped.
	unit	-

- cache_hit_ratio_percent

  - Settings (initial status)

Member		Setting (initial status)
name		cache_hit_ratio_percent
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		(1 - (rate(oracledb_activity_physical_reads_cache[2m]) / (rate(oracledb_activity_consistent_gets_from_cache[2m]) +rate(oracledb_activity_db_block_gets_from_cache[2m]))))*100 and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Cache Hit Ratio
	description	Shows the cache hit ratio.
	unit	%

- tablespace_used_percent

  - Settings (initial status)

Member		Setting (initial status)
name		tablespace_used_percent
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		oracledb_tablespace_used_percent and $jp1im_TrendData_labels
resource_en	category	database_oracle

Member		Setting (initial status)
	label	Tablespace Usage
	description	Shows the usage of each tablespace. If automatic extension is ON, it is calculated based on the size considering automatic extension.
	unit	%

- execute_count
  - Settings (initial status)

Member		Setting (initial status)
name		execute_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		rate(oracledb_activity_execute_count[2m])*60 and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	SQL Statement Execution Count
	description	Shows the number of calls to execute SQL statements (user calls and recursive calls).
	unit	-

- parse_count
  - Settings (initial status)

Member		Setting (initial status)
name		parse_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		rate(oracledb_activity_parse_count_total[2m])*60 and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Parsing Call Execution Count
	description	Shows the execution count of parsing calls (hard, soft, and describe).
	unit	-

- user_commit_count
  - Settings (initial status)

Member		Setting (initial status)
name		user_commit_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		rate(oracledb_activity_user_commits[2m])*60 and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Commit Execution Count
	description	Shows the number of user commits.
	unit	-

- user_rollback_count
  - Settings (initial status)

Member		Setting (initial status)
name		user_rollback_count
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		rate(oracledb_activity_user_rollbacks[2m])*60 and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Rollback Execution Count
	description	Shows the number of times users issued a ROLLBACK statement manually or the number of errors occurred in user transactions.
	unit	-

- resource_used
  - Settings (initial status)

Member		Setting (initial status)
name		resource_used
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		oracledb_resource_current_utilization and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Resource Usage
	description	Shows the resource usage.
	unit	-

- session_count
  - Settings (initial status)

Member		Setting (initial status)
name		session_count
default		false
promql for the metric definition file (including $jp1im_TrendData_labels)		oracledb_sessions_value and $jp1im_TrendData_labels
resource_en	category	database_oracle
	label	Number of Sessions
	description	Shows the number of sessions based on status and type.
	unit	-

OracleDB exporter default collection metric definition file (default-metrics.toml)

Format

A TOML format file.

See GitHub website for the format of this file.

File

`default_metrics.toml`

`default_metrics.toml.model` (model file)

Storage directory

- Integrated agent host (model files only)

In Windows:

- For a physical host

Windows versions of OracleDB exporter archived file # are extracted to `\oracledb_exporter_windows\conf\`

#

Agent path`\options\oracledb_exporter_windows_`**VVRRSS**`.zip`

In Linux:

- For a physical host

Linux versions of OracleDB exporter archived file # are extracted to `/oracledb_exporter_linux/conf/`

#

`/opt/jp1ima/options/oracledb_exporter_linux_`**VVRRSS**`.tar.gz`

Description

Files that define metric that OracleDB exporter retrieves.

This file cannot be edited.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This is applied when OracleDB exporter is started or restarted.

Description

See GitHub website for the format of this file.

Container monitoring metric definition file (metrics_kubernetes.conf)

Syntax

```
[
  {
    "name":"metric-name-of-trend-data",
    "default":default-selection-status,
    "promql":"PromQL-statement",
    "resource_en":{
      "category":"metric-category-in-English",
      "label":"metric-label-in-English",
      "description":"metric-description-in-English",
      "unit":"metric-unit-in-English"
    },
    "resource_ja":{
      "category":"metric-category-in-Japanese",
      "label":"metric-label-in-Japanese",
      "description":"metric-description-in-Japanese",
      "unit":"metric-unit-in-Japanese"
    },
    "module": "component-name"
  }, ...
]#
```

#

The number of elements that can be written inside the brackets (`[]`) is from 1 to 1,000. A KAJY24609-E error message is output when writing a number of elements that falls outside this range.

File

`metrics_kubernetes.conf`

`metrics_kubernetes.conf.model` (Model file)

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs_kubernetes\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs_kubernetes\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs_kubernetes/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs_kubernetes/`

Description

This file defines the container monitoring metric information shown in the **Trends** tab of the Integrated Operation Viewer window.

Definitions are used for the return values of the __metricListGet method and __timeSeriesDataGet method for JP1/IM - Agent product plug-ins. If JP1/IM - Manager is in a hierarchical configuration and trend data stored in the database of a lower-level manager is referenced from an upper-level manager, you must add the metrics of the referenced trend data to the metrics definition file of the upper-level manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected when metric information is retrieved in the **Trends** tab on the Integrated Operation Viewer window, or in the REST API.

Content description

For details, see *Content description* in *Node exporter metric definition file (metrics_node_exporter.conf) (2. Definition Files)* for JP1/IM - Agent. However, the `module` member is required and the component type is specified. The value specified here is used as the object root type.

Settings in the model file (initial status)

The following shows the settings (initial status) of each metric written in the container monitoring metric definition file (model file).

- kube_job_status_failed
  - Settings (initial status)

Member		Setting (initial status)
name		kube_job_status_failed
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		kube_job_status_failed * on(job_name, namespace) group_left() kube_job_owner{owner_kind=\"<none>\", owner_name=\"<none>\"} and $jp1im_TrendData_labels
resource_en	category	kubernete_job
	label	Number of Failed pods
	description	The number of pods which reached Phase Failed and the reason for failure. This number does not include pods run from a CronJob.
	unit	count
module		kubernetes/Namespace

- kube_pod_status_pending

- Settings (initial status)

Member		Setting (initial status)
name		kube_pod_status_pending
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_pod_status_phase{phase=\"Pending\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Number of Pending pods
	description	The number of pods whose Phase is Pending.
	unit	count
module		kubernetes/Namespace

- kube_pod_status_failed
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_status_failed
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_pod_status_phase{phase=\"Failed\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Number of Failed pods
	description	The number of pods whose Phase is Failed.
	unit	count
module		kubernetes/Namespace

- kube_pod_status_unknown
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_status_unknown
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_pod_status_phase{phase=\"Unknown\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Number of Unknown pods
	description	The number of pods whose Phase is Unknown.
	unit	count
module		kubernetes/Namespace

- kube_daemonset_failed_number_scheduled
  - Settings (initial status)

Member		Setting (initial status)
name		kube_daemonset_failed_number_scheduled
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		(kube_daemonset_status_desired_number_scheduled - kube_daemonset_status_current_number_scheduled) and $jp1im_TrendData_labels
resource_en	category	kubernetes_daemon_set
	label	Number of nodes failed to run
	description	The difference between the number of nodes that need to run daemon pods (desired) and the number of nodes that are already running (current).
	unit	count
module		kubernetes/DaemonSet

- kube_deployment_failed_replicas
  - Settings (initial status)

Member		Setting (initial status)
name		kube_deployment_failed_replicas
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		(kube_deployment_spec_replicas - kube_deployment_status_replicas_available) and $jp1im_TrendData_labels
resource_en	category	kubernetes_deploymen
	label	Number of pods failed to run
	description	The difference between the number of required pods and the number of available replicas.
	unit	count
module		kubernetes/Deployment

- kube_replicaset_failed_replicas
  - Settings (initial status)

Member		Setting (initial status)
name		kube_replicaset_failed_replicas
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		(kube_replicaset_spec_replicas - kube_replicaset_status_ready_replicas) and $jp1im_TrendData_labels
resource_en	category	kubernetes_replica_set
	label	Number of pods failed to run
	description	The difference between the number of required pods and the number of ready replicas.
	unit	count
module		kubernetes/ReplicaSet

- kube_statefulset_failed_replicas
  - Settings (initial status)

Member		Setting (initial status)
name		kube_statefulset_failed_replicas
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		(kube_statefulset_replicas - kube_statefulset_status_replicas_ready) and $jp1im_TrendData_labels
resource_en	category	kubernetes_stateful_set
	label	Number of pods failed to run
	description	The difference between the number of required pods and the number of ready replicas.
	unit	count
module		kubernetes/StaetfulSet

- kube_cron_job_status_failed
  - Settings (initial status)

Member		Setting (initial status)
name		kube_cron_job_status_failed
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		kube_job_status_failed * on(job_name, namespace) group_left(jp1_pc_nodelabel) kube_job_owner{owner_kind=\"CronJob\", owner_name!=\"<none>\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_cron_job
	label	Number of pods failed to run
	description	The number of pods that failed to run within a CronJob.
	unit	count
module		kubernetes/CronJob

- kube_node_status_condition_not_ready
  - Settings (initial status)

Member		Setting (initial status)
name		kube_node_status_condition_not_ready
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (node, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_node_status_condition{condition=\"Ready\",status=~\"false|unknown\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_node
	label	Status
	description	Whether the node is in an error state. (1: Not Ready or Unknown, 0: Ready)
	unit	count
module		kubernetes/Node

- kube_node_status_condition_memory_pressure
  - Settings (initial status)

Member		Setting (initial status)
name		kube_node_status_condition_memory_pressure
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (node, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_node_status_condition{condition=\"MemoryPressure\",status=~\"true|unknown\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_node
	label	Memory pressure
	description	Whether memory is under pressure. (1: Under Pressure or Unknown, 0: Normal)
	unit	count
module		kubernetes/Node

- kube_node_status_condition_disk_pressure
  - Settings (initial status)

Member		Setting (initial status)
name		kube_node_status_condition_disk_pressure
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (node, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_node_status_condition{condition=\"DiskPressure\",status=~\"true|unknown\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_node
	label	Disk pressure
	description	Whether disk is under pressure. (1: Under Pressure or Unknown, 0: Normal)
	unit	count
module		kubernetes/Node

- kube_node_status_condition_pid_pressure
  - Settings (initial status)

Member		Setting (initial status)
name		kube_node_status_condition_pid_pressure
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (node, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (kube_node_status_condition{condition=\"PIDPressure\",status=~\"true|unknown\"} and $jp1im_TrendData_labels)
resource_en	category	kubernetes_node
	label	PID pressure
	description	Whether PID is under pressure. (1: Under Pressure or Unknown, 0: Normal)
	unit	count
module		kubernetes/Node

- kube_pod_cpu_percent_used
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_cpu_percent_used
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_cpu_usage_seconds_total{name!=""}[2m]) and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	CPU usage
	description	CPU usage per pod.
	unit	%
module		kubernetes/Namespace

- kube_pod_fs_reads_bps
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_fs_reads_bps
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_reads_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Disk read bytes
	description	Disk read bytes per pod.
	unit	Bps
module		kubernetes/Namespace

- kube_pod_fs_writes_bps
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_fs_writes_bps
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_writes_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Disk write bytes
	description	Disk write bytes per pod.
	unit	Bps
module		kubernetes/Namespace

- kube_pod_memory_percent_used
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_memory_percent_used
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (container_memory_working_set_bytes and (container_spec_memory_limit_bytes{name!=""} > 0) and $jp1im_TrendData_labels) / sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) ((container_spec_memory_limit_bytes{name!=""} > 0) and container_memory_working_set_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	Memory usage
	description	Memory usage per pod.
	unit	%
module		kubernetes/Namespace

- kube_namespace_cpu_percent_used
  - Settings (initial status)

Member		Setting (initial status)
name		kube_namespace_cpu_percent_used
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_cpu_usage_seconds_total{name!=""}[2m]) and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	CPU usage
	description	CPU usage per namespace.
	unit	%
module		kubernetes/Cluster

- kube_namespace_fs_reads_bps
  - Settings (initial status)

Member		Setting (initial status)
name		kube_namespace_fs_reads_bps
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_reads_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Disk read bytes
	description	Disk read bytes per namespace.
	unit	Bps

Member		Setting (initial status)
module		kubernetes/Cluster

- kube_namespace_fs_writes_bps
  - Settings (initial status)

Member		Setting (initial status)
name		kube_namespace_fs_writes_bps
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_writes_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Disk write bytes
	description	Disk write bytes per namespace.
	unit	Bps
module		kubernetes/Cluster

- kube_namespace_memory_percent_used
  - Settings (initial status)

Member		Setting (initial status)
name		kube_namespace_memory_percent_used
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (container_memory_working_set_bytes and (container_spec_memory_limit_bytes{name!=""} > 0) and $jp1im_TrendData_labels) / sum by (namespace, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) ((container_spec_memory_limit_bytes{name!=""} > 0) and container_memory_working_set_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	Memory usage
	description	Memory usage per namespace.
	unit	%
module		kubernetes/Cluster

- kube_pod_status_phase
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_status_phase
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		kube_pod_status_phase and $jp1im_TrendData_labels
resource_en	category	kubernetes_pod

Member		Setting (initial status)
	label	Phase
	description	The pods current phase
	unit	-
module		kubernetes/Pod

- kube_pod_cpu_percent_used_pod
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_cpu_percent_used_pod
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_cpu_usage_seconds_total{name!=""}[2m]) and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	CPU usage
	description	CPU usage per pod.
	unit	%
module		kubernetes/Pod

- kube_pod_fs_reads_bps_pod
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_fs_reads_bps_pod
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_reads_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)
resource_en	category	kubernetes_pod
	label	Disk read bytes
	description	Disk read bytes per pod.
	unit	Bps
module		kubernetes/Pod

- kube_pod_fs_writes_bps_pod
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_fs_writes_bps_pod
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (rate(container_fs_writes_bytes_total{name!=""}[2m]) and $jp1im_TrendData_labels)

Member		Setting (initial status)
resource_en	category	kubernetes_pod
	label	Disk write bytes
	description	Disk write bytes per pod.
	unit	Bps
module		kubernetes/Pod

- kube_pod_memory_percent_used
  - Settings (initial status)

Member		Setting (initial status)
name		kube_pod_memory_percent_used_pod
default		true
promql for the metric definition file (including $jp1im_TrendData_labels)		sum by (namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) (container_memory_working_set_bytes and (container_spec_memory_limit_bytes{name!=""} > 0) and $jp1im_TrendData_labels) / sum by (pod, namespace, instance, job, jp1_pc_nodelabel, jp1_pc_prome_hostname) ((container_spec_memory_limit_bytes{name!=""} > 0) and container_memory_working_set_bytes and $jp1im_TrendData_labels) * 100
resource_en	category	kubernetes_pod
	label	Memory usage
	description	Memory usage per pod.
	unit	%
module		kubernetes/Pod

Any Prometheus trend name metric definition file (metrics_any-Prometheus-trend-name.conf)

Format

See the *Format* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_`*any-Prometheus-trend-name*`.conf`

The *any-Prometheus-trend-name* should be a Value that Setup the `jp1_pc_trendname` of the discovery configuration file or Prometheus configuration file.

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

This File defines metric to be displayed on the [Trend] tabbed page of Integrated Operation Viewer window.

Defined content is used for the __metricListGet method of product plugin in JP1/IM - Agent and the return Value of the __timeSeriesDataGet method.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This is reflected when metric is acquired on the [Trend] tab of Integrated Operation Viewer window or REST API.

Information that is specified

See the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

User-specific metric definition file (metrics_any-Prometheus-trend-name.conf)

Format

See the *Format* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_`*any-Prometheus-trend-name*`.conf`

Set *any-Prometheus-trend-name* to the value that is setup to the `jp1_pc_trendname` of the user-specific discovery configuration file.

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\user\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\user\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/user/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/user/`

Description

This file defines the user specific metric information which displayed in the **Trend** tab of Integration Operation Viewer window.

Definition uses a return value of `__metricListGet` method and `__timeSeriesDataGet` method in the product plug-in of JP1/IM - Agent.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition File of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

The definitions take effect when execute .`__metricListGet` method or `__timeSeriesDataGet` method in the product plug-in of JP1/IM - Agent.

Information that is specified

See the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

User-specific metric definition file (Promitor) (metrics_*any-Prometheus-trend-name*.conf)

Syntax

See the *Format* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

File

`metrics_`*any-Prometheus-trend-name*`.conf`

Set *any-Prometheus-trend-name* to the value that is setup to the `jp1_pc_trendname` of the user-specific discovery configuration file.

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs_azure\user\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs_azure\user\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs_azure/user/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs_azure/user/`

Description

This file defines the user specific metric information which displayed in the **Trend** tab of Integration Operation Viewer window.

Definition uses a return value of `__metricListGet` method and `__timeSeriesDataGet` method in the product plug-in of JP1/IM - Agent.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition File of Integrated manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

The definitions take effect when execute .`__metricListGet` method or `__timeSeriesDataGet` method in the product plug-in of JP1/IM - Agent.

Content description

See the *Information that is specified* section in *Node exporter metric definition file (metrics_node_exporter.conf)*.

User-specific metric definition file (container monitoring) (metrics_*any-Prometheus-trend-name*.conf)

Syntax

See the *Format* section in *Container monitoring metric definition file (metrics_kubernetes.conf)*.

File

`metrics_`*any-Prometheus-trend-name*`.conf`

Set *any-Prometheus-trend-name* to the value that is setup to the `jp1_pc_trendname` of the user-specific discovery configuration file.

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs_kubernetes\user\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs_kubernetes\user\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs_kubernetes/user/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs_kubernetes/user/`

Description

This file defines the user specific metric information which displayed in the **Trend** tab of Integration Operation Viewer window.

Definition uses a return value of `__metricListGet` method and `__timeSeriesDataGet` method in the product plug-in of JP1/IM - Agent.

If JP1/IM - Manager is in a hierarchical configuration and you want to refer to trend data stored in Trend data Management Database of lower manager from Integrated manager, you must add trend data metrics that you want to refer to metric definition File of Integrated manager.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows; CR+LF

In Linux: LF

Timing in which definitions are reflected

The definitions take effect when execute .__metricListGet method or __timeSeriesDataGet method in the product plug-in of JP1/IM - Agent.

Content description

See the *Information that is specified* section in *Container monitoring metric definition file (metrics_kubernetes.conf)*.

AWS definition file (aws_settings.conf)

Format

```
{
  "yace_account_mapping": {
    "AWS Account ID":"AWS account string",
    ...
  }
}
```

File

`aws_settings.conf`

`aws_settings.conf.model` (model file)

Storage directory

■Integrated manager host

In Windows:

- For a physical host
  Manager-path`\conf\imdd\plugin\jp1pccs\`
- For a logical host
  shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs\`

In Linux:

- For a physical host
  `/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs/`
- For a logical host
  shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs/`

Description

Configuration files for AWS and Yet another cloudwatch exporter.

Set it when monitoring using the Yet another cloudwatch exporter in the monitoring module (Cloud).

yace_account_mapping specifies the mapping between the AWS account ID used by Yet another cloudwatch exporter and the account string to be set in the IM management node properties and extended attribute values of the JP1 event. If there is no corresponding definition for the account ID specified in Yet another cloudwatch exporter, the IM management node properties of the Yet another cloudwatch exporter and the account in the extended attribute value of the JP1 event are set to "default".

If JP1/IM - Manager is in a hierarchical configuration and lower manager manages Yet another cloudwatch exporter, you must specify the mapping of AWS account ID of Yet another cloudwatch exporter managed by lower manager and the account string set in properties of IM managed node or JP1 event extension to AWS definition file of Integrated manager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the jddcreatetree and jddupdatetree commands are executed, they are reflected in the tree display contents of the Integrated Operations Viewer. Or, an alert that monitors Yet another cloudwatch exporter's performance data reflects when the JP1 event is issued.

Information that is specified

AWS Account ID

Specify the AWS account ID to be used in the settings for connecting to CloudWatch from Yet another cloudwatch exporter, using characters other than 1 to 255 control characters.

For CloudWatch connection Setup, see *2.19.2(7)(b) Modify Setup to connect to CloudWatch (for Linux) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

AWS account string

Specify the SID of Yet another cloudwatch exporter and the account string to be set for the account in the properties of the IM management node in characters other than 1 to 255 control characters.

Alertmanager configuration file (jpc_alertmanager.yml)

Format

Write in YAML format.

```
  :
(Abbreviated)
  :
receivers:
- name: 'JP1IMDD'

  webhook_configs:
  - send_resolved: true
    url: 'http://host-name-of-JP1/IM - Agent:20726/ima/api/v1/proxy/service/
imdd/im/api_system/v1/events/transform'
```

File

`jpc_alertmanager.yml`

`jpc_alertmanager.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This is a configuration file that defines the operation of AlertManager.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflected when Alertmanager is restarted and when Alertmanager is instructed to reload.

Information that is specified

For definitions of common placeholders used in the table below, see *About definition of common placeholders for descriptive items in yml file*.

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
global:		--	N	--	--
route: <route>		Configure alert routing. See the <route> description below.	Y	For details, see <route> below.	--
receivers:		Set the notification destination for the alert.	N	--	--
	- <receiver> ...	See the <receiver> description below.	Y	For details, see <receiver> below.	Describes the definition for sending to JP1/IM - Manager (Intelligent Integrated Management Platform).

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- <route>

Set only one for sending to the Integrated Operations Viewer for JP1/IM.

Item	Description	Change ability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
[receiver: <string>]	Specify the value of name in the definition of the alert notification destination set for receivers.	N	--	receiver: 'JP1IMDD'
[group_by: '[' <labelname>, ... ']']	Specify if you want to group multiple alerts from the Prometheus server by label. Specify ['...'] to disable grouping.	N	--	group_by: ['...']
[continue: <boolean> | default = false]	Specifies whether to continue routing alerts.	N	--	continue: false
[group_wait: <duration> | default = 30s]	Specify the amount of time to wait for grouping alerts. Group alerts that arrived during the waiting time.	N	--	group_wait: 5s
[group_interval: <duration> | default = 5m]	Specifies the interval before snoozing when a new alert is added to a group of alerts.	N	--	group_interval: 5s
[repeat_interval: <duration> | default = 4h]	Specify the interval after which an alert is notified before snoozing. If you specify a value greater than the period specified in the command line option --data.retention, you may be soldered earlier than the period specified in the repeat_interval.	N	--	repeat_interval: 7d

Legend:

N: Not changeable, --: Not applicable

- <receiver>

Item	Description	Change ability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
name: <string>	Specifies the name of the alert notification destination setting.	N	--	- name: 'JP1IMDD'
webhook_configs:	--	N	--	--
[send_resolved: <boolean> | default = true]	Specifies whether to notify recovery alerts. <Configuration Example> See receivers.webhook_configs.url.	Y	Specify false if you do not want to be notified of recovery.	- send_resolved: true
url: <string>	Specify the endpoint to which you want to be notified of alerts. <Configuration Example> receivers: - name: 'JP1IMDD' webhook_configs: - send_resolved: true url: 'http://localhost:20726/ima/api/v1/proxy/service/imdd/im/api/v1/events/transform'	R	Specify imagent endpoints on the same host. Modify Host name and Port number to suit your deployment.	url: 'http://*integrated-agent-host-name*:20726/ima/api/v1/proxy/service/imdd/im/api/v1/events/transform'

Legend:

R: Required, Y: Changeable, N: Not changeable, --: Not applicable

Prometheus configuration file (jpc_prometheus_server.yml)

Format

Write in YAML format.

```
global:
  scrape_interval:      1m
  scrape_timeout:      10s
  evaluation_interval:  1m
  external_labels:
    jp1_pc_prome_hostname: "Monitoring agent host name"
  :
(Abbreviated)
  :
scrape_configs:#
  - job_name: Scrape Job Name

    file_sd_configs:
      - files:
        - Discovery configuration file name

    relabel_configs:
      - target_label: jp1_pc_nodelabel
        replacement: Node exporter
      - regex: (jp1_pc_category|jp1_pc_trendname)
        action: labeldrop
  :
(Abbreviated)
  :
remote_write:
  - url: http://host-name-of-JP1/IM - Agent:20727/ima/api/v1/proxy/service/p
romscale/api/v1/write
    remote_timeout: 30s
    send_exemplars: false
    queue_config:
      capacity: 10000
      max_shards: 200
      min_shards: 4
      max_samples_per_send: 3000
      batch_send_deadline: 10s
      min_backoff: 100ms
      max_backoff: 10s
```

#

When Script exporter discovery is specified using the HTTP-based *http_sd_config* method, specify the direct endpoint to http_sd_configs.url in scrape_configs in this file.

The following shows the HTTP-based service discovery endpoint for the Script exporter specified in http_sd_configs.url in scrape_configs.

```
http://installation-host-name:Script-exporter-port-number/discovery
```

In contrast to file_sd_configs, labels cannot be independently added with http_sd_configs. Labels must be added using relabel_configs. For details on the labels required, see *1.21.2(10)(b) Scraping definition for Script exporter* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

File

`jpc_prometheus_server.yml`

`jpc_prometheus_server.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This is a configuration file that defines the operation of the Prometheus server.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When you run the Prometheus server reload API or restart the Prometheus server, it is reflected in the operation of the Prometheus server.

Also, if the value of the jp1_pc_prome_hostname label or the scrape definition (definition of the scrape_configs) is changed, it will be reflected in the displayed contents of the tree in the integrated operation viewer when the jddcreatetree command and the jddupdatetree command are executed after performing the above operation.

Information that is specified

For definitions of common placeholders used in the table below, see *About definition of common placeholders for descriptive items in yml file*.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
global:	--	N	--	--
[scrape_interval: <duration> | default = 1m]	Specify the scrape interval to the target, ranging from 15 seconds to 24 hours. The value is specified in numbers and units. The units that can be specified are s (seconds), m (minutes), and h (hours). <Configuration Example> global: scrape_interval: 5m	Y	Specifies the scrape interval.#	scrape_interval:1m
[scrape_timeout: <duration> | default = 10s]	Specifies the scrape request timeout period, ranging from 10 seconds to 60 minutes. The value is specified in numbers and units. The units that can be specified are s (seconds) and m (minutes). You must specify a value that is less than global.scrape_interval. <Configuration Example> global: scrape_timeout: 20s	Y	Configure as needed.	scrape_timeout: 10s
[evaluation_interval: <duration> | default = 1m]	Specify the evaluation interval for the alert rule, ranging from 15 seconds to 48 hours. The value is specified in numbers and units. You can specify the following units: s (seconds), m (minutes), and h (hours). <Configuration Example> global: evaluation_interval: 15s	Y	Configure as needed.	evaluation_interval : 1m
external_labels:	Specify a label to add when notifying remote lights and Alertmanager. You can specify up to 30 of them.	N	--	--
[<labelname>: <labelvalue> ...]	Specify the label name and label value. The label name and label value can be up to 255 bytes each. Do not delete jp1_pc_prome_hostname labels that are set by default. <Configuration Example> global: external_labels: labelname1: valuename1 labelname2: valuename2	Y	Since it is set by the installation script of the monitoring module, it is usually not necessary to change it. In a clustered environment, manually set the logical host name.	external_labels: jp1_pc_prome_hostname: "*host-name*"
rule_files:	Specify the alert rule file. You can specify up to 30 of them.	N	--	--
[- <filepath_glob> ...]	Specify a file name. The file name can be up to 255 bytes. <Configuration Example> rule_files: - " jpc_alerting_rules.yml" - "alerting_rules2.yml"	Y	You can change, add, and delete rule file names. Normally, no changes are required.	rule_files: - "jpc_alerting_rules.yml"

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
scrape_configs:	Specifies the scrape definition. You can specify up to 30 of them.	N	--	--
[- <scrape_config> ...]	See the description of <scrape_config> below.	Y	You can add scrape definitions. If you have your own Exporter, add a definition. Normally, no changes are required.	The following Exporter definitions are pre-populated: • node_exporter • windows_exporter • blackbox_exporter(http) • blackbox_exporter(icmp) • yet_another_cloudwatch_exporter
alerting:	Configure the settings related to Alertmanager.	N	--	--
alert_relabel_configs:	Set up relabeling for alert notifications.	N	--	--
[- <relabel_config> ...]	See the description of <relabel_config> below.	Y	Specify this if you want to add or change the label of the alert.	--
alertmanagers:	Configure the alert notification destination Alertmanager.	N	--	--
[- <alertmanager_config> ...]	See the description of <alertmanager_config> below.	Y	Specify the cohabiting Alertmanager as the alert notification destination.	--
remote_write:	Configure settings related to remote writing.	N	--	--
url: <string>	Specify the endpoint to which the remote write is sent. <Configuration Example> remote_write: - url: http://*integrated-agent-host-name*:20727/ima/api/v1/proxy/service/promscale/write	R	Specifies the remote write endpoint for imagent on the same host. Modify Host name and Port number to suit your needs.	url: http://localhost:20727/ima/api/v1/proxy/service/promscale/write
[remote_timeout: <duration> | default = 30s]	Specify the remote write timeout period in the range of 30 seconds to 60 minutes. The value is specified in numbers and units. The units that can be specified are s (seconds) and m (minutes). <Configuration Example> remote_write: - url: http://localhost:20727/ima/api/v1/proxy/service/promscale/write remote_timeout: 1m	Y	If the remote write times out, increase the value.	remote_timeout: 30s
write_relabel_configs:	Set up relabeling during remote write.	N	--	--

Item			Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
		[- <relabel_config> ...]	See the description of <relabel_config> below. <Configuration Example> The following is a setting example when you do not want to remotely write the node_boot_time_seconds and node_context_switches_total obtained by node_exporter command. remote_write: - url: http://localhost:20727/ima/api/v1/proxy/service/promscale/write write_relabel_configs: - source_labels: ['__name__'] regex: '(node_boot_time_seconds|node_context_switches_total)' action: 'drop'	Y	Specify if you do not want to remotely write a specific metric.	--
	[send_exemplars: <boolean> | default = false]		Specify to write Exemplars remotely.	N	--	send_exemplars: false
	queue_config:		Set up a queue for remote write.	N	--	--
		[capacity: <int> | default = 2500]	Specifies the number of samples to buffer.	N	--	capacity: 10000
		[min_shards: <int> | default = 1]	Specify the lower limit for the number of parallel executions of remote write.	N	--	min_shards: 4
		[max_samples_per_send: <int> | default = 500]	Specifies the maximum number of samples to send at one time.	N	--	max_samples_per_send: 3000
		[batch_send_deadline: <duration> | default = 5s]	Specifies the amount of time to wait before flushing the remaining queued samples.	N	--	batch_send_deadline: 10s
		[min_backoff: <duration> | default = 30ms]	Specifies the minimum wait time limit for transmission retries.	N	--	min_backoff: 100ms
		[max_backoff: <duration> | default = 100ms]	Specifies the upper limit of the wait time for transmission retries.	N	--	max_backoff: 10s

Legend:

R: Required, Y: Changeable, N: Not changeable, --: Not applicable

#

When changing this value from the initial value (1m), review the value of the range vector selector specified in the PromQL statement of the metric definition file (the time range specified by square brackets { }). For the range vector selector, specify a value that is at least twice the scrape interval. If you specify a value less than 2 times, trend information cannot be obtained or trend information cannot be obtained at some times.

Also, when monitoring using Yet another cloudwatch exporter, do not specify a value greater than 10m. If specified, the configuration may not be retrieved when the jddcreatetree command is executed.

- <scrape_config>

  scrape_config section specifies a set of parameters that describe targets and how to scrape them.

  In general, one job is specified in one scrape configuration. In advanced configurations, this is subject to change.

  Targets can be statically configured via static_configs parameters or dynamically discovered using one of the supported service discovery mechanisms.

In addition, relabel_configs allows you to make advanced changes to targets and their labels before scraping.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
job_name: <job_name>	Specifies the name of the scrape definition. This value is set to the job label in the performance data. The job name cannot exceed 255 characters. • For user-defined Exporter Specify a jobname that does not start with "jpc". However, if Exporter is the same as Exporter provided by JP1/IM - Agent, specify it by referring to <job_name> below. • For container monitoring See *1.21.2(11) Setting up container monitoring* in the *JP1/Integrated Management 3 - Manager Configuration Guide*. <Configuration Example> scrape_configs: - job_name: 'my_exporter'	Y	If you use your own Exporter, define a new scrape job name.	The following jobs are configured: • jpc_node • jpc_windows • jpc_blackbox_http • jpc_blackbox_icmp • jpc_cloudwatch
[scrape_interval: <duration> | default = <global_config.scrape_interval>]	Specifies the amount of time between scrape to the destination, from 15 seconds to 24 hours. Specify this if you want the interval to be different from the scrape interval specified for the global.scrape_interval. The value is specified in numbers and units. Possible units are s (seconds), m (minutes), and h (hours). <Configuration Example> scrape_configs: - job_name: 'my_exporter' scrape_interval: 10m	Y	Specify if you want to change global and the scrape interval. If the value of job_name is "jpc_cloudwatch", do not specify a value greater than 10m. If specified, the configuration may not be retrieved when the jddcreatetree command is executed.	--
[scrape_timeout: <duration> | default = <global_config.scrape_timeout>]	Specifies the scrape request timeout period, ranging from 10 seconds to 60 minutes. The value is specified in numbers and units. The units that can be specified are s (seconds) and m (minutes). When this value is omitted, the value is going to be the smaller value of scrape_config.scrape_interval and global.scrape_timeout. <Configuration Example> scrape_configs: - job_name: 'my_exporter' scrape_timeout: 30s	Y	Specify this if you want to change the global and scrape timeout periods.	--
[metrics_path: <path> | default = /metrics]	Specifies the HTTP resource path to scrape within 255 bytes. If not specified, "/metrics" is added to the URL at the time of scrape. <Configuration Example>	Y	Specify if you want to use your own Exporter.	Specify the path for each job.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	scrape_configs: - job_name: 'my_exporter' metrics_path: /sample-metrics			
[scheme: <scheme> | default = http]	Specifies the protocol to use for the request. You can specify "http" or "https". <Configuration Example> scrape_configs: - job_name: 'my_exporter' scheme: https	Y	Specify "http" or "https" to match the exporter.	--
params:	Specify HTTP URL parameters when scraping. You can specify up to 30 of them.	Y	--	--
[<string>: [<string>, ...]]	Specify the key and value. The key and value can be up to 255 bytes each. <Configuration Example> scrape_configs: - job_name: 'my_exporter' params: aaa: [bbb, ccc] xxx: [yyy]	Y	Specify the URL parameters to pass to the exporter when scraping to match the exporter.	--
file_sd_configs:	Defines the file for which you want to set the scrape target.	N	--	--
-files:	Specifies the file to be scraped.	N	--	--
[- <filename_pattern> ...]	Specify a file name of up to 255 characters. <Configuration Example> scrape_configs: - job_name: 'my_exporter' file_sd_configs: - files: - 'file_sd_config_my_exporter.yml'	Y	Specify if you want to use your own Exporter. To use the following functions in an environment upgraded from 13-00, the user must change the settings manually. • Node exporter for AIX For details on changing the settings, see *Setting up Node exporter for AIX scrape jobs* in *1.23.2(1)(c) Setting Up JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.	For each job, make the following definitions. - 'jpc_file_sd_config_node.yml' - 'jpc_file_sd_config_windows.yml' - 'jpc_file_sd_config_blackbox_http.yml' - 'jpc_file_sd_config_blackbox_icmp.yml' - 'jpc_file_sd_config_cloudwatch.yml' - 'jpc_file_sd_config_node_aix.yml'
[refresh_interval: <duration> | default = 5m]	Specify the interval between reloading files containing scrape targets, ranging from 5 minutes to 24 hours. The value is specified in numbers and units. You can specify the following units: m (minutes) and h (hours).	Y	Specify this if you want to change the reload interval for files when using your own exporter.	--

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
		<Configuration Example> scrape_configs: - job_name: 'my_exporter' file_sd_configs: - files: - 'file_sd_config_my_exporter.yml' refresh_interval: 10m		Normally, no changes are required.	
relabel_configs:		Sets the relabeling for the target before scraping.	N	--	--

	[- <relabel_config> ...]	See the description of <relabel_config> below.	Y	Specify if you want to use your own Exporter.
				To use the following functions in an environment upgraded from 13-00, the user must change the settings manually.
				• Node exporter for AIX
				For details on on changing the settings, see *Setting up Node exporter for AIX scrape jobs* in *1.23.2(1)(c) Setting Up JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.
					The following definitions are made for each job.
					• For jpc_node
					`- target_label: jp1_pc_nodelabel`
					`replacement: Linux metric collector(Node exporter)`
					• For jpc_windows
					`- target_label: jp1_pc_nodelabel`
					`replacement: Windows metric collector(Windows exporter)`
					• For jpc_blackbox_http
					`- source_labels: [__address__]`
					`target_label: __param_target`
					`regex: ([^:]+):([^:]+):(.*)`
					`replacement: ${3}`
					`- source_labels: [__address__]`
					`target_label: instance`
					`- source_labels: [__address__]`
					`target_label: jp1_pc_nodelabel`
					`regex: ([^:]+):([^:]+):(.*)`

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value

					`replacement: ${2}`
					`- target_label: __address__`
					`replacement: integrated agent host name:20715`
					`- source_labels: [__param_module]`
					`target_label: jp1_pc_module`
					• For jpc_blackbox_icmp
					`- source_labels: [__address__]`
					`target_label: __param_target`
					`- target_label: jp1_pc_nodelabel`
					`replacement: Synthetic metric collector(Blackbox exporter(ICMP))`
					`- source_labels: [__address__]`
					`target_label: instance`
					`- target_label: __address__`
					`replacement: integrated agent host name:20715`
					`- source_labels: [__param_module]`
					`target_label: jp1_pc_module`
					• For jpc_cloudwatch
					It is not necessary to state.
					• For jpc_node_aix

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value

				`- target_label: jp1_pc_nodelabel`
				`replacement: AIX metric collector(Node exporter for AIX)`

metric_relabel_configs:	Set up relabeling for metrics after scraping. For setting examples, see the explanation of "write_relabel_configs:" in item "remote_write:".	N	--	--
[- <relabel_config> ...]	See the description of <relabel_config> below.	Y	Specify this option in the following cases: • When to Use user-defined Exporter • You want to remove a particular metric. • When metric is labeled by monitoring the operation rate of processes[#2] or other means To use the following functions in an environment upgraded from JP1/IM - Agent 13-00 to 13-01 or later, the user must change the settings manually. • Service monitoring function • Node exporter for AIX • For details on changing the settings, see *1.21.2(3)(f) Configuring service monitoring settings (For Windows) (Optional)* and *2.19.2(3)(f) Setting up service monitoring (for Linux) (Optional)* and *1.23.2(1)(c) Setting up JP1/IM - Agent* in the *JP1/ Integrated Management 3 - Manager*	Specify the exporter relabel for each job.[#]

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
				Configuration Guide.	

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

#

- In case of jpc_node:

  - source_labels: ['__name__']

  regex: 'node_network_receive_bytes_total|node_network_transmit_bytes_total|
  node_disk_read_time_seconds_total|node_disk_write_time_seconds_total|node_boot_time_seconds|
  node_context_switches_total|node_cpu_seconds_total|node_disk_io_now|node_disk_io_time_seconds_total|
  node_disk_read_bytes_total|node_disk_reads_completed_total|node_disk_writes_completed_total|
  node_disk_written_bytes_total|node_filesystem_avail_bytes|node_filesystem_files|
  node_filesystem_files_free|node_filesystem_free_bytes|node_filesystem_size_bytes|node_intr_total|
  node_load1|node_load15|node_load5|node_memory_Active_file_bytes|node_memory_Buffers_bytes|
  node_memory_Cached_bytes|node_memory_Inactive_file_bytes|node_memory_MemAvailable_bytes|
  node_memory_MemFree_bytes|node_memory_MemTotal_bytes|node_memory_SReclaimable_bytes|
  node_memory_SwapFree_bytes|node_memory_SwapTotal_bytes|node_netstat_Icmp6_InMsgs|
  node_netstat_Icmp_InMsgs|node_netstat_Icmp6_OutMsgs|node_netstat_Icmp_OutMsgs|
  node_netstat_Tcp_InSegs|node_netstat_Tcp_OutSegs|node_netstat_Udp_InDatagrams|
  node_netstat_Udp_OutDatagrams|node_network_flags|node_network_iface_link|node_network_mtu_bytes|
  node_network_receive_errs_total|node_network_receive_packets_total|node_network_transmit_colls_total|
  node_network_transmit_errs_total|node_network_transmit_packets_total|node_time_seconds|
  node_uname_info|node_vmstat_pswpin|node_vmstat_pswpout | node_systemd_unit_state'

  action: 'keep'

  - source_labels: ['__name__']

  regex: 'node_systemd_unit_.*'

  target_label: 'jp1_pc_trendname'

  replacement: 'node_exporter_service'

  - source_labels: ['__name__']

  regex: 'node_systemd_unit_.*'

  target_label: 'jp1_pc_category'

  replacement: 'service'

  - source_labels: ['__name__','name']

  regex: 'node_systemd_unit_.*;(.*)'

  target_label: 'jp1_pc_nodelabel'

  replacement: ${1}

  - regex: jp1_pc_multiple_node

  action: labeldrop

- In case of jpc_windows:

  - source_labels: ['__name__']

  regex: 'windows_cs_physical_memory_bytes|windows_cache_copy_read_hits_total|
  windows_cache_copy_reads_total|windows_cpu_time_total|windows_logical_disk_free_bytes|
  windows_logical_disk_idle_seconds_total|windows_logical_disk_read_bytes_total|

```
windows_logical_disk_read_latency_seconds_total|windows_logical_disk_read_seconds_total|
windows_logical_disk_reads_total|windows_logical_disk_requests_queued|
windows_logical_disk_size_bytes|windows_logical_disk_write_bytes_total|
windows_logical_disk_write_latency_seconds_total|windows_logical_disk_write_seconds_total|
windows_logical_disk_writes_total|windows_memory_available_bytes|windows_memory_cache_bytes|
windows_memory_cache_faults_total|windows_memory_page_faults_total|
windows_memory_pool_nonpaged_allocs_total|windows_memory_pool_paged_allocs_total|
windows_memory_swap_page_operations_total|windows_memory_swap_pages_read_total|
windows_memory_swap_pages_written_total|windows_memory_system_cache_resident_bytes|
windows_memory_transition_faults_total|windows_net_bytes_received_total|windows_net_bytes_sent_total|
windows_net_bytes_total|windows_net_packets_sent_total|windows_net_packets_received_total|
windows_system_context_switches_total|windows_system_processor_queue_length|
windows_system_system_calls_total | windows_process_start_time | windows_process_cpu_time_total |
windows_process_handles | windows_process_io_bytes_total | windows_process_io_operations_total |
windows_process_page_faults_total | windows_process_page_file_bytes | windows_process_pool_bytes |
windows_process_priority_base | windows_process_private_bytes | windows_process_threads |
windows_process_virtual_bytes | windows_process_working_set_private_bytes |
windows_process_working_set_peak_bytes | windows_process_working_set_bytes | windows_service_state'
action: 'keep'
- source_labels: ['__name__']
regex: 'windows_process_.*'
target_label: 'jp1_pc_trendname'
replacement: 'windows_exporter_process'
- source_labels: ['__name__','process']
regex: 'windows_process_.*;(.*)'
target_label: 'jp1_pc_nodelabel'
replacement: ${1}
- source_labels: ['__name__']
regex: 'windows_service_.*'
target_label: 'jp1_pc_trendname'
replacement: 'windows_exporter_service'
- source_labels: ['__name__']
regex: 'windows_service_.*'
target_label: 'jp1_pc_category'
replacement: 'service'
- source_labels: ['__name__','name']
regex: 'windows_service_.*;(.*)'
target_label: 'jp1_pc_nodelabel'
replacement: ${1}
- regex: jp1_pc_multiple_node
action: labeldrop
```

- In case of jpc_blackbox_http:

```
- source_labels: ['__name__']
regex: 'probe_http_duration_seconds|
probe_http_content_length|probe_http_uncompressed_body_length|probe_http_redirects|probe_http_ssl|
probe_http_status_code|probe_ssl_earliest_cert_expiry|probe_ssl_last_chain_expiry_timestamp_seconds|
probe_ssl_last_chain_info|probe_tls_version_info|probe_http_version|probe_failed_due_to_regex|
probe_http_last_modified_timestamp_seconds|probe_success|probe_duration_seconds'
action: 'keep'
```

- In case of jpc_blackbox_icmp:

  ```
  - source_labels: ['__name__']
  regex: 'probe_icmp_duration_seconds|probe_icmp_reply_hop_limit|probe_success|probe_duration_seconds'
  action: 'keep'
  ```

- In case of jpc_cloudwatch:

  ```
  - regex: 'tag_(jp1_pc_.*)'
  replacement: ${1}
  action: labelmap
  - regex: 'tag_(jp1_pc_.*)'
  action: 'labeldrop'
  - source_labels: ['__name__','jp1_pc_nodelabel']
  regex: '(aws_ec2_cpuutilization_average|aws_ec2_disk_read_bytes_sum|aws_ec2_disk_write_bytes_sum|
  aws_lambda_errors_sum|aws_lambda_duration_average|aws_s3_bucket_size_bytes_sum|
  aws_s3_5xx_errors_sum|aws_dynamodb_consumed_read_capacity_units_sum|
  aws_dynamodb_consumed_write_capacity_units_sum|aws_states_execution_time_average|
  aws_states_executions_failed_sum|aws_sqs_approximate_number_of_messages_delayed_sum|
  aws_sqs_number_of_messages_deleted_sum | aws_ebs_volume_read_bytes_sum |
  aws_ebs_volume_write_bytes_sum | aws_ecs_cpuutilization_average |
  aws_ecs_memory_utilization_average | aws_efs_total_iobytes_average | aws_efs_storage_bytes_average |
  aws_fsx_data_read_bytes_sum | aws_fsx_data_write_bytes_sum | aws_fsx_free_storage_capacity_average |
  aws_rds_cpuutilization_average | aws_rds_read_iops_average | aws_rds_write_iops_average |
  aws_sns_number_of_notifications_failed_sum | aws_sns_number_of_notifications_filtered_out_sum);.+$'
  action: 'keep'
  - source_labels: ['__name__','dimension_ClusterName']
  target_label: jp1_pc_nodelabel
  regex: 'aws_ecs_.+;(.+)'
  replacement: ${1}
  - source_labels: ['__name__','dimension_ServiceName']
  target_label: jp1_pc_nodelabel
  regex: 'aws_ecs_.+;(.+)'
  replacement: ${1}
  ```

- For jpc_process

  ```
  - source_labels: [groupname]
  regex: ([^;]*?);([^;]*?);(.*)
  target_label: program
  replacement: ${1}
  - source_labels: [groupname]
  regex: ([^;]*?);([^;]*?);(.*)
  target_label: user
  replacement: ${2}
  - source_labels: [groupname]
  regex: ([^;]*?);([^;]*?);(.*)
  ```

```
target_label: command_line
replacement: ${3}
- source_labels: [program]
target_label: jp1_pc_nodelabel
- source_labels: ['__name__']
regex: 'namedprocess_namegroup_num_procs | namedprocess_namegroup_cpu_seconds_total |
namedprocess_namegroup_read_bytes_total | namedprocess_namegroup_write_bytes_total |
namedprocess_namegroup_major_page_faults_total | namedprocess_namegroup_minor_page_faults_total |
namedprocess_namegroup_context_switches_total | namedprocess_namegroup_memory_bytes |
namedprocess_namegroup_open_filedesc | namedprocess_namegroup_worst_fd_ratio |
namedprocess_namegroup_oldest_start_time_seconds | namedprocess_namegroup_num_threads |
namedprocess_namegroup_states | namedprocess_namegroup_thread_count |
namedprocess_namegroup_thread_cpu_seconds_total | namedprocess_namegroup_thread_io_bytes_total |
namedprocess_namegroup_thread_major_page_faults_total |
namedprocess_namegroup_thread_minor_page_faults_total |
namedprocess_namegroup_thread_context_switches_total'
action: 'keep'
- regex: (jp1_pc_multiple_node | jp1_pc_agent_create_flag)
action: labeldrop
```

- For jpc_promitor

```
- source_labels: [resource_uri]
regex: ([^/]+)/([^/]+)/([^/]+)/([^/]+)/([^/]+)/([^/]+)/([^/]+)/(.*)
target_label: jp1_pc_nodelabel
replacement: ${8}
- source_labels: ['__name__']
regex: 'azure_virtual_machine_disk_read_bytes_total | azure_virtual_machine_disk_write_bytes_total |
azure_virtual_machine_percentage_cpu_average | azure_blob_storage_availability_average |
azure_blob_storage_blob_capacity_average | azure_function_app_http5xx_total |
azure_function_app_http_response_time_average | azure_cosmos_db_total_request_units_total |
azure_logic_app_runs_failed_total | azure_container_instance_cpu_usage_average |
azure_container_instance_memory_usage_average |
azure_kubernetes_service_kube_pod_status_phase_average | azure_file_storage_availability_average |
azure_file_storage_file_capacity_average | azure_service_bus_namespace_deadlettered_messages_average |
azure_sql_database_cpu_percent_average | azure_sql_database_dtu_used_average |
azure_sql_database_storage_maximum | azure_sql_elastic_pool_cpu_percent_average |
azure_sql_elastic_pool_e_dtu_used_average | azure_sql_elastic_pool_storage_used_average |
azure_sql_managed_instance_avg_cpu_percent_average |
azure_sql_managed_instance_io_bytes_read_average |
azure_sql_managed_instance_io_bytes_written_average |
azure_sql_managed_instance_storage_space_used_mb_average'
action: 'keep'
- regex: jp1_pc_rm_agent_create_flag
action: labeldrop
- source_labels: ['__name__','phase']
regex: (azure_kubernetes_service_kube_pod_status_phase_average);Failed
target_label: __name__
replacement: ${1}_failed
```

- source_labels: ['__name__','phase']
regex: (azure_kubernetes_service_kube_pod_status_phase_average);Pending
target_label: __name__
replacement: ${1}_pending
- source_labels: ['__name__','phase']
regex: (azure_kubernetes_service_kube_pod_status_phase_average);Unknown
target_label: __name__
replacement: ${1}_unknown

- For jpc_script
  - source_labels: ['__name__']
  regex: 'script_success | script_duration_seconds | script_exit_code'
  action: 'keep'
  - source_labels: [jp1_pc_script]
  target_label: jp1_pc_nodelabel
  - regex: (jp1_pc_script | jp1_pc_multiple_node | jp1_pc_agent_create_flag)
  action: labeldrop
- For jpc_node_aix
  - source_labels: ['__name__']
  regex: 'node_context_switches | node_cpu | aix_diskpath_wblks | aix_diskpath_rblks | aix_disk_rserv | aix_disk_rblks | aix_disk_wserv | aix_disk_wblks | aix_disk_time | aix_disk_xrate | aix_disk_xfers | node_filesystem_avail_bytes | node_filesystem_files | node_filesystem_files_free | node_filesystem_free_bytes | node_filesystem_size_bytes | node_intr|node_load1 | node_load5 | node_load15 | aix_memory_real_avail | aix_memory_real_free | aix_memory_real_inuse | aix_memory_real_total | aix_netinterface_mtu | aix_netinterface_ibytes | aix_netinterface_ierrors | aix_netinterface_ipackets | aix_netinterface_obytes | aix_netinterface_collisions | aix_netinterface_oerrors | aix_netinterface_opackets | aix_memory_pgspins | aix_memory_pgspouts'
  action: 'keep'

- <job_name>
  Specify the job name (same as the scrape job name specified by JP1/IM - Agent's Prometheus configuration file) shown in the following tables if user-defined Exporter is the same as Exporter provided by JP1/IM - Agent.

Exporter Name	Job name to specify
Node exporter	jpc_node
Windows exporter	jpc_windows
Node exporter for AIX	jpc_node_aix
Blackbox exporter	jpc_blackbox_http or jpc_blackbox_icmp
Yet another cloudwatch exporter	jpc_cloudwatch
Process exporter	jpc_process
Promitor	jpc_promitor
Script exporter	Job name starts with "jpc_script"

- <static_config>
  The static_config allows you to set a list of targets and a set of labels that are common to them. This is a typical way to specify a static target in a scrape configuration.

Note: In the JP1/IM - Agent, it is described in the file specified in the file_sd_config.

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
targets:		Specifies the scrape target. You can specify up to 100.	N	--	--
	[- '<host>']	Specifies the host name to be scraped within 255 bytes. <Configuration Example> - targets: - HOST1:1000 - HOST2:2000	Y	Specifies the scrape target.	--
labels:		Specify the label that you want to set for all metrics retrieved from scrape. You can specify up to 30 of them.	N	--	--
	[<labelname>: <labelvalue> ...]	Specify the label name and label value. The label name and label value can be up to 255 bytes each.	Y	Specify if you want to add a label to the metric.	--

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- <relabel_config>

  You can configure relabel_config to edit target labels or exclude specified targets before processing scrapes, remote lights, alert notifications, and so on.

  relabel_config settings are applied to each target in the order in which they appear in the configuration file.

  Initially, the following labels are set for the target:

  - For the target job label, the value of the job_name of each scrape definition is set.
  - The instance label and __address__ label are set to the string specified in the targets of the discovery configuration file.
  - If __param_ [name] label exists in the target, the URL parameter of the form "[*name*]=*value*" is set when scraping.
  - The target is set to the label specified in labels in the discovery configuration file.

  Since Prometheus server scrapes the "host name: port number" set in the __address__ label, if the value specified for targets is not the "host name: port number" to scrape destination, it is necessary to edit the scrape definition by relabel_config.

  Labels beginning with __ are removed from the data after processing such as scraping, remote light, and alert notifications.

  If the relabel step needs to store the label value temporarily (as input to subsequent relabel steps), use the __tmp label name prefix. This prefix is guaranteed not to be used by Prometheus itself.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
[source_labels: '[' <labelname> [, ...] ']']	For Source label, select a value from an existing label. The contents are concatenated using the configured separator and matched against	Y	Same as the "Description" column.	--

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	the regular expressions configured for the replace, keep, and drop actions.			
[separator: <string> | default = ;]	Sets the separator that is placed between the values of the concatenated source label.	Y	Same as the "Description" column.	--
[target_label: <labelname>]	Sets the label to which the replacement action writes the resulting value. Required for replace actions. Regex capture groups are available.	Y	Same as the "Description" column.	--
[regex: <regex> | default = (.*)]	Sets the regular expression against which the extracted values are matched. For details, see the <regex> explanation below.	Y	Same as the "Description" column.	--
[replacement: <string> | default = $1]	Sets the replacement value at which the regular expression substitution is performed if the regular expression matches. Regex capture groups are available.	Y	Same as the "Description" column.	--
[action: <relabel_action> | default = replace]	Sets the action to take based on regular expression matching. For details, see <relabel_action> below.	Y	Same as the "Description" column.	--

Legend:

Y: Changeable, --: Not applicable

- <regex>

  Set any valid RE2 regular expression.

  Required for replace, keep, drop, and labeldrop actions. Regex is anchored at both ends. To unanchor a regular expression, use .*[regex].*.

- <relabel_action>

  Set the relabeling action.

  replace:

  Match regex against concatenated source_labels. and the matchgroup reference (${1}, ${2}, ...) with that value, and set the target_label to replacement. If the regex does not match, replacement is not performed.

  keep:

  Remove targets that do not match the regex concatenated source_labels.

  drop:

  Deletes targets that match the regex concatenated source_labels.

  labeldrop:

  Match regex to all label names. The matched label is removed from the set of labels.

  Configuration Example: User's own scrape definition

  If you use your own exporter and define multiple monitoring targets in the discovery configuration file, you must specify `regex` for the `relabel_config` and set the value to the `jp1_pc_nodelabel`.

  For scrape defined setup and `jp1_pc_nodelabel`, see *1.21.2(3)(d) Add user-defined Exporter scrape job (for Windows) (optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

The following three monitoring targets are set in the `targets` of the discovery configuration file. Set "`target1 label`", "`target2 label`", and "`target3 label`" to the `jp1_pc_nodelabel` as the label name of each IM management node.

```
- targets:
  - hostA:target1 label:query-parameter-1-passed-to-exporter
  - hostA:target2 label:query-parameter-2-passed-to-exporter
  - hostB:target3 label:query-parameter-3-passed-to-exporter
```

Specifying relabel_config

```
relabel_configs:
 - source_labels:[__address__]     +
   target_label:__param_target     | (1)
   regex:([^:]+):([^:]+):(.*)      |
   replacement:${3}                +
 - source_labels:[__address__]     + (2)
   target_label:instance           +
 - source_labels:[__address__]     + (3)
   target_label:jp1_pc_nodelabel   |
   regex:([^:]+):([^:]+):(.*)      |
   replacement:${2}                +
 - target_label:__address__        + (4)
   replacement:localhost:20799     +
```

(1): The value set in `__address__` (`hostA:target1 label:`*query-parameter-1-passed-to-Exporter*) is split, and the string of *query-parameter-1-passed-to-Exporter* is set to the `__param_target` label. `target` is the URL parameter when scraping.

(2):I am setting the `instance` label to the value set for `__address__`.

(3): The value set in `__address__` is split, and the label name (`target`*X* `label`) of the IM management node is set to the `jp1_pc_nodelabel` label.

(4): The user's own exporter scrape destination information (*host-name* : *port-number*) is set in the `__address__`.

- <metric_relabel_configs>

  `Metric relabeling` is applied to the sample as the last step before ingestion. It has the same configuration format and action as `Target relabeling`. `Metric relabeling` does not apply to automatically generated time series such as `up`.

  This is used to filter out time series that are too expensive to ingest.

- <alert_relabel_configs>

  `Alert relabeling` applies to alerts before they are sent to AlertManager.

  It has the same configuration format and action as `target relabeling`. Alert relabeling is applied after the external label.

  One use use is to ensure that HA pairs of Prometheus servers with different external labels send the same alert.

- <alertmanager_config>

  `alertmanager_config` section specifies the Alertmanager instance to which the Prometheus server sends alerts. It also provides parameters to set how to communicate with these Alertmanagers.

  Alertmanager can also be statically set with `static_configs` parameters or dynamically discovered using one of the supported service discovery mechanisms.

Item			Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
static_configs:			Configure the settings by direct specification.	N	--	--
	- targets:		Specifies the Alertmanager to which the alert should be sent.	N	--	--
		[- '<host>']	Specify the host name up to 255 bytes. <Configuration Example> alerting: alertmanagers: - static_configs: - targets: [*integrated-agent-host-name*:20714]	R	For the port number, specify the port of Alertmanager. If a host name or internet address is specified for --web.listen-address in the Alertmanager command line option, modify localhost to the host name or internet address specified in --web.listen-address.	localhost:20714

Legend:

R: Required, N: Not changeable, --: Not applicable

Alert configuration file (jpc_alerting_rules.yml)

Format

Write in YAML format.

```
groups:
  - name: group-name
    rules:
    - alert: alert-name
      expr: Conditional expressions
      for: Period
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: JP1 event severity
        jp1_pc_eventid: Event ID of the JP1 event
        jp1_pc_metricname: Metric Name
      annotations:
        jp1_pc_firing_description: Message when firing conditions are met
        jp1_pc_resolved_description: Message when a firing condition is no l
onger met
```

File

`jpc_alerting_rules.yml`

`jpc_alerting_rules.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

A file that defines the alert evaluation rules that the Prometheus server runs.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflected when the Prometheus server is restarted and when you instruct the Prometheus server to reload.

Information that is specified

For definitions of common placeholders used in the table below, see *About definition of common placeholders for descriptive items in yml file*.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
groups:	--	N	--	"groups:"
name: <string>	Specify the alert group name within 255 bytes. The group name must be unique within the monitoring agent host, and you cannot specify multiple names with the same group name. Note that between different monitoring agent hosts, you can specify a name that specifies the same group name for each.	Y	Specify a group name of your choice.	Not specified
rules:	Configure alert rules. You can specify up to 100.	N	--	Not specified
alert: <string>	Specify a name for the alert.	Y	Specifies the name of the alert created by the user.	Not specified
expr: <string>	Specify the alert expression within 255 bytes. Specifies the PromQL statement.	Y	Specifies the PromQL statement to evaluate.# For notes on PromQL statements, see *Note on PromQL expression*.	Not specified
for: <duration>	Specify the duration for an alert to become firing, ranging from 0 seconds to 24 hours. The value is specified in numbers and units. The units that can be specified are s (seconds) and m (minutes). Even if the alert condition expression is applicable, if it no longer applies within the period specified for `for`, it will not be treated as firing.	Y	Specifies the amount of time it takes for an alert to reach a firing state.	Not specified
labels:	Set labels to add or override for each alert.	N	--	Not specified
jp1_pc_product_name: <string>	Specify the value to be set for the product name of the JP1 event.	Y	"/HITACHI/JP1/JPCCS2", or "/HITACHI/JP1/JPCCS2/xxxx" You can specify xxxx.	Not specified
jp1_pc_component: <string>	Specify the value to be set for the component name of the JP1 event.	Y	Depending on the product plug-in that handles the JP1 event, specify the following values.	Not specified

Item				Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
						jp1pccs_azure.js:"/HITACHI/JP1/JPCCS/AZURE/CONFINFO" jp1pccs_kubernetes.js:"/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO" jp1pccs.js:"/HITACHI/JP1/JPCCS/CONFINFO"	
			jp1_pc_severity: <string>	Specify the value to set for the severity of the JP1 event.	Y	Specify one of the following: • Emergency • Alert • Critical • Error • Warning • Notice • Information • Debug	Not specified
			jp1_pc_eventid: <string>	Specify the value to be set for the event ID of the JP1 event.	Y	Specify any value in the range of "0 to 1FFF,7FFF8000 to 7FFFFFFF" that can be specified as the event ID of the JP1 event.	If the specification is omitted, "00007600" is Setup to Value of ID property of JP1 event.
			jp1_pc_metricname: <string>	Specify the value to be set for the metric name of the JP1 event. In the case of Yet another cloudwatch exporter, the JP1 event is associated with the IM management node in the AWS namespace corresponding to the metric name (or the first metric name if multiple comma-separated values are specified).	Y	Specify the metric names separated by commas.	Not specified
		annotations:		Set the annotations that you want to add to each alert.	N	--	Not specified
			jp1_pc_firing_description: <string>	Specify the value to be set for the message of the JP1 event when the firing condition of the alert is satisfied. If the length of the value is 1,024 bytes or more, set the string from the beginning to the 1,023rd byte. If the specification is omitted, the message content of the JP1 event is "The alert is firing. (alert = *alert name*)".	Y	Specify an optional message.	If the specification is omitted, the message content of the JP1 event is "The alert is firing. (alert = *alert name*)".
			jp1_pc_resolved_description: <string>	Specify the value to be set for the JP1 event message when the firing condition of the alert is no longer satisfied. If the length of the value is 1,024 bytes or more, set the string from the beginning to the 1,023rd byte. If the specification is omitted, the content of the message in the JP1 event is "The alert is resolved. (alert = *alert name*)".	Y	Specify an optional message.	If the specification is omitted, the content of the message in the JP1 event is "The alert is resolved. (alert = *alert name*)".

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

#

Since the following label is set as an attribute of the JP1 event, do not remove the label by an aggregate operator.

- instance
- job
- jp1_pc_nodelabel
- jp1_pc_exporter
- jp1_pc_remote_monitor_instance
- account
- region
- dimension_*any-string*

Note that the labels accout, region, and dimension_*any-string* apply only when monitoring Yet another cloudwatch exporter metrics.

Definition example

The following shows an example of an alert definition for each metric written in the model file of the metric definition file.

■Metric alert definition example in *Node exporter metric definition file*

- cpu_used_rate#

```
groups:
  - name: node_exporter
    rules:
    - alert: cpu_used_rate(Node exporter)
      expr: 80 < (avg by (instance,job,jp1_pc_nodelabel,jp1_pc_exporter) (
rate(node_cpu_seconds_total{mode="system"}[2m])) + avg by (instance,job,jp
1_pc_nodelabel,jp1_pc_exporter) (rate(node_cpu_seconds_total{mode="user"}[
2m]))) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0301"
        jp1_pc_metricname: "node_cpu_seconds_total"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%)."
```

- memory_unused#

```
groups:
  - name: node_exporter
    rules:
    - alert: memory_unused(Node exporter)
      expr: 1024 > node_memory_MemAvailable_bytes/1024/1024
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0302"
        jp1_pc_metricname: "node_memory_MemAvailable_bytes"
      annotations:
        jp1_pc_firing_description: "The amount of free memory has fallen b
elow the threshold (1024 megabytes).value={{ $value }}megabytes"
        jp1_pc_resolved_description: "The amount of free memory exceeded t
he threshold (1024 megabytes)."
```

- memory_unused_rate#

```
groups:
  - name: node_exporter
    rules:
    - alert: memory_unused_rate(Node exporter)
      expr: node_memory_MemAvailable_bytes  / node_memory_MemTotal_bytes
* 100 < 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0302"
        jp1_pc_metricname: "node_memory_MemAvailable_bytes,node_memory_Mem
Total_bytes"
      annotations:
        jp1_pc_firing_description: "Free-memory ratio has fallen below thr
eshold value (10%). value={{$value}} %"
        jp1_pc_resolved_description: "Free-memory ratio exceeded threshol
d value (10%). "
```

- disk_unused#

```
groups:
  - name: node_exporter
    rules:
    - alert: disk_unused(Node exporter)
      expr: 10 > node_filesystem_free_bytes/(1024*1024*1024)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0303"
        jp1_pc_metricname: "node_filesystem_free_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk space has fallen below the t
hreshold (10 gigabytes).value={{ $value }}gigabytes, mountpoint={{ $labels
.mountpoint }}"
        jp1_pc_resolved_description: "Free disk space exceeded threshold (
10 gigabytes).mountpoint={{ $labels.mountpoint }}"
```

- disk_unused_rate#

```
groups:
  - name: node_exporter
    rules:
    - alert: disk_unused_rate(Node exporter)
      expr: node_filesystem_free_bytes / node_filesystem_size_bytes * 100
< 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0303"
        jp1_pc_metricname: "node_filesystem_free_bytes,node_filesystem_siz
e_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk percentage has fallen below
threshold value (10%). value={{$value}} %, mountpoint={{$labels.mountpoint
}}"
        jp1_pc_resolved_description: "Free disk percentage exceeds thresho
ld value (10%). mountpoint={{$labels.mountpoint}}"
```

Note

If you want to monitor both Node exporter and Node exporter for AIX on a single Prometheus, specify `job` labels in `expr` of the `disk_unused` of Node exporter alert definition to distinguish between metric for Node exporter and Node exporter for AIX, as shown in the underlined part below.

```
10 > node_filesystem_free_bytes{job="jpc_node"}/ (1024*1024*1024)
```

- disk_busy_rate#

```
groups:
  - name: node_exporter
    rules:
    - alert: disk_busy_rate(Node exporter)
      expr: 70 < rate(node_disk_io_time_seconds_total[2m])*100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0304"
        jp1_pc_metricname: "node_disk_io_time_seconds_total"
      annotations:
        jp1_pc_firing_description: "Disk busy rate exceeded threshold (70%
).value={{ $value }}%, device={{ $labels.device }}"
        jp1_pc_resolved_description: "Disk busy rate has fallen below the
threshold (70%).device={{ $labels.device }}"
```

Note

If you want to monitor both Node exporter and Node exporter for AIX on a single Prometheus, specify `job` labels in `expr` of the `disk_unused_rate` of Node exporter alert definition to distinguish between metric for Node exporter and Node exporter for AIX, as shown in the underlined part below.

```
Node_filesystem_free_bytes{job="jpc_node"} /
node_filesystem_size_bytes{job="jpc_node"} * 100 < 10
```

- disk_read_latency#

```
groups:
  - name: node_exporter
    rules:
    - alert: disk_read_latency(Node exporter)
      expr: rate(node_disk_read_time_seconds_total[2m]) / rate(node_disk_r
eads_completed_total[2m]) > 0.1 and rate(node_disk_reads_completed_total[2
m]) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0304"
        jp1_pc_metricname: "node_disk_read_time_seconds_total,node_disk_re
ads_completed_total"
      annotations:
        jp1_pc_firing_description: "Disk read latency exceeds the threshol
d Value (0.1 seconds). value={{$value}}s, device={{$labels.device}}"
        jp1_pc_resolved_description: "Disk read latency has fallen below t
hreshold Value (0.1 seconds). device={{$labels.device}}"
```

- disk_write_latency#

```
ggroups:
  - name: node_exporter
    rules:
    - alert: disk_write_latency(Node exporter)
      expr: rate(node_disk_write_time_seconds_total[2m]) / rate(node_disk_
writes_completed_total[2m]) > 0.1 and rate(node_disk_writes_completed_tota
l[2m]) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0304"
        jp1_pc_metricname: "node_disk_write_time_seconds_total,node_disk_w
rites_completed_total"
      annotations:
        jp1_pc_firing_description: "Disc write latency exceeds the thresho
ld Value (0.1 sec.). value={{$value}}%, device={{$labels.device}}"
        jp1_pc_resolved_description: "Disc write latency has fallen below
threshold value (0.1 seconds). device={{$labels.device}}"
```

- disk_io_latency#

```
groups:
  - name: node_exporter
    rules:
    - alert: disk_io_latency(Node exporter)
      expr: (rate(node_disk_read_time_seconds_total[2m]) + rate(node_disk_
write_time_seconds_total[2m])) / (rate(node_disk_reads_completed_total[2m]
) + rate(node_disk_writes_completed_total[2m])) > 0.1 and (rate(node_disk_
writes_completed_total[2m]) > 0 or rate(node_disk_read_completed_total[2m]
) > 0)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0304"
        jp1_pc_metricname: "node_disk_write_time_seconds_total,node_disk_w
rites_completed_total,node_disk_read_time_seconds_total,node_disk_reads_co
mpleted_total"
      annotations:
        jp1_pc_firing_description: "Disk IO latency exceeded the threshol
d Value (0.1 seconds). value={{$value}}%, device={{$labels.device}}"
        jp1_pc_resolved_description: "Disc IO latency has fallen below thr
eshold value (0.1 seconds). device={{$labels.device}}"
```

- network_sent#

```
groups:
  - name: node_exporter
    rules:
    - alert: network_sent(Node exporter)
      expr: 100 < rate(node_network_transmit_packets_total[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0305"
        jp1_pc_metricname: "node_network_transmit_packets_total"
      annotations:
        jp1_pc_firing_description: "The network transmission speed exceede
d the threshold (100 packets per second). value={{ $value }}packets per se
cond, device={{ $labels.device }}"
        jp1_pc_resolved_description: "The network transmission speed has d
ropped below the threshold (100 packets per second). device={{ $labels.dev
ice }}"
```

- network_received#

```
groups:
  - name: node_exporter
    rules:
    - alert: network_received(Node exporter)
      expr: 100 < rate(node_network_receive_packets_total[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0306"
        jp1_pc_metricname: "node_network_receive_packets_total"
      annotations:
        jp1_pc_firing_description: "The network receive speed exceeded th
e threshold (100 packets per second).value={{ $value }}packets per second
, device={{ $labels.device }}"
        jp1_pc_resolved_description: "The network receive speed has droppe
d below the threshold (100 packets per second).device={{ $labels.device }
}"
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "`groups:`" or duplicate `name` with the same group-name.

■Metric alert definition example in *Process exporter metric definition file*

- process_pgm_process_count#

```
groups:
  - name: process_exporter
    rules:
    - alert: process_pgm_process_count(Processs exporter)
      expr: 1 >  sum by (program, instance, job, jp1_pc_nodelabel, jp1_pc_
exporter) (namedprocess_namegroup_num_procs)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1308"
        jp1_pc_metricname: "namedprocess_namegroup_num_procs"
      annotations:
        jp1_pc_firing_description: "The number of processes has fallen bel
ow the threshold (1 process)."
        jp1_pc_resolved_description: "The number of processes has exceede
d the threshold (1 process)."
```

#

This uses a threshold value of 1 as an example. Change this value based on the number of monitoring targets.

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate.

- Alert definition example for metrics in "Node exporter (service monitoring) metric definition file"

- service_state#

  When the auto-start setting of the monitored unit is enabled (systemctl enable is being executed)

```
groups:
  - name: node_exporter
    rules:
    - alert: service_state(Node exporter)
      expr: node_systemd_unit_state{state="active"} == 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0320"
        jp1_pc_metricname: "node_systemd_unit_state"
      annotations:
        jp1_pc_firing_description: "The status of the service is not runni
ng."
        jp1_pc_resolved_description: "The service status is now running."
```

When the auto-start setting of the monitored unit is disabled

```
groups:
  - name: node_exporter
```

```
    rules:
    - alert: service_state_service-name(Node exporter)
      expr: absent(node_systemd_unit_state{instance="integrated-agent-host
-name:port-number-of-the-Node-exporter", job="jpc_node", jp1_pc_exporter="
JPC Node exporter", jp1_pc_nodelabel="service-name", state="active"}) == 1
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0320"
        jp1_pc_metricname: "node_systemd_unit_state"
      annotations:
        jp1_pc_firing_description: "The status of the service is not runni
ng."
        jp1_pc_resolved_description: "The service status is now running."
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "groups:" or duplicate name with the same group-name.

■Metric alert definition example in *Windows exporter metric definition file*

- cpu_used_rate#

```
groups:
  - name: windows_exporter
    rules:
    - alert: cpu_used_rate(Windows exporter)
      expr: 80 < 100 - (avg by (instance,job,jp1_pc_nodelabel,jp1_pc_expor
ter) (rate(windows_cpu_time_total{mode="idle"}[2m])) * 100)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0401"
        jp1_pc_metricname: "windows_cpu_time_total"
      annotations:
        jp1_pc_firing_description: "CPU utilization exceeded threshold (80
%).value={{ $value }}%"
        jp1_pc_resolved_description: "CPU usage has dropped below the thre
shold (80%)."
```

- memory_unused#

```
groups:
  - name: windows_exporter
    rules:
    - alert: memory_unused(Windows exporter)
      expr: 1 > windows_memory_available_bytes/1024/1024/1024
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0402"
        jp1_pc_metricname: "windows_memory_available_bytes"
      annotations:
        jp1_pc_firing_description: "The amount of free memory has fallen b
elow the threshold (1 gigabytes).value={{ $value }}Gb"
        jp1_pc_resolved_description: "The amount of free memory exceeded t
he threshold (1 gigabytes)."
```

- memory_unused_rate#

```
groups:
  - name: windows_exporter
    rules:
    - alert: memory_unused_rate(Windows exporter)
      expr: windows_memory_available_bytes / windows_cs_physical_memory_by
tes * 100 < 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0402"
        jp1_pc_metricname: "windows_memory_available_bytes,windows_cs_phys
ical_memory_bytes"
      annotations:
        jp1_pc_firing_description: "Free-memory ratio has fallen below thr
eshold value (10%). value={{$value}} %"
        jp1_pc_resolved_description: "Free-memory ratio exceeded threshol
d value (10%)."
```

- disk_unused#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_unused(Windows exporter)
      expr: 10 > windows_logical_disk_free_bytes{volume!~"HarddiskVolume.*
"} / (1024*1024*1024)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0403"
        jp1_pc_metricname: "windows_logical_disk_free_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk space has fallen below the t
hreshold (10 gigabytes).value={{ $value }}GB, volume={{ $labels.volume }}"
        jp1_pc_resolved_description: "Free disk space exceeded threshold (
10 gigabytes).volume={{ $labels.volume }}"
```

- disk_unused_rate#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_unused_rate(Windows exporter)
      expr: windows_logical_disk_free_bytes{volume!~"HarddiskVolume.*"} /
windows_logical_disk_size_bytes * 100 < 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0403"
        jp1_pc_metricname: "windows_logical_disk_free_bytes,windows_logica
l_disk_size_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk percentage has fallen below
threshold value (10%). value={{$value}}%, volume={{$labels.volume}}"
        jp1_pc_resolved_description: "Free disk percentage exceeds thresho
ld value (10%). volume={{$labels.volume}}"
```

- disk_busy_rate#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_busy_rate(Windows exporter)
      expr: 70 < 100 - rate(windows_logical_disk_idle_seconds_total{volume
!~"HarddiskVolume.*"}[2m])/(rate(windows_logical_disk_write_seconds_total[
2m]) + rate(windows_logical_disk_read_seconds_total[2m])+rate(windows_logi
cal_disk_idle_seconds_total[2m])) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0404"
        jp1_pc_metricname: "windows_logical_disk_idle_seconds_total,windo
ws_logical_disk_write_seconds_total,windows_logical_disk_read_seconds_tota
l"
      annotations:
        jp1_pc_firing_description: "Disk busy rate exceeded threshold (70%
).value={{ $value }}%, volume={{ $labels.volume }}"
        jp1_pc_resolved_description: "The disk busy rate has fallen below
the threshold (70%).volume={{ $labels.volume }}"
```

- disk_read_latency#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_read_latency(Windows exporter)
      expr: rate(windows_logical_disk_read_seconds_total[2m] / rate(window
s_logical_disk_reads_total[2m]) > 0.1 and rate(windows_logical_disk_reads_
total[2m]) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0404"
        jp1_pc_metricname: "windows_logical_disk_read_seconds_total,window
s_logical_disk_reads_total"
      annotations:
        jp1_pc_firing_description: "Disk read latency exceeds the threshol
d Value (0.1 seconds). value={{$value}}s, volume={{$labels.volume}}"
```

```
        jp1_pc_resolved_description: "Disk read latency has fallen below t
hreshold value (0.1 seconds). volume={{$labels.volume}}"
```

- disk_write_latency#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_write_latency(Windows exporter)
      expr: rate(windows_logical_disk_write_seconds_total[2m] / rate(windo
ws_logical_disk_writes_total[2m]) > 0.1 and rate(windows_logical_disk_writ
es_total[2m]) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0404"
        jp1_pc_metricname: "windows_logical_disk_write_seconds_total,windo
ws_logical_disk_writes_total"
      annotations:
        jp1_pc_firing_description: "Disk write latency exceeds the thresho
ld Value (0.1 sec.). value={{$value}}s, volume={{$labels.volume}}"
        The jp1_pc_resolved_description: "Disk write latency has fallen be
low the threshold value (0.1 seconds). volume={{$labels.volume}}"
```

- disk_io_latency#

```
groups:
  - name: windows_exporter
    rules:
    - alert: disk_io_latency(Windows exporter)
      expr: (rate(windows_logical_disk_read_seconds_total[2m]) + rate(wind
ows_logical_disk_write_seconds_total[2m])) / (rate(windows_logical_disk_re
ads_total[2m]) + rate(windows_logical_disk_writes_total[2m])) > 0.1 and (r
ate(windows_logical_disk_writes_total[2m]) > 0 or rate(windows_logical_dis
k_reads_total[2m]) > 0)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0404"
        jp1_pc_metricname: "windows_logical_disk_write_seconds_total,windo
ws_logical_disk_writes_total,windows_logical_disk_read_seconds_total,windo
ws_logical_disk_reads_total"
      annotations:
        jp1_pc_firing_description: "Disk IO latency exceeded the threshol
d Value (0.1 seconds). value={{$value}}s, volume={{ $labels.volume }}"
        jp1_pc_resolved_description: "Disk IO latency has fallen below th
e threshold value (0.1 seconds). volume={{ $labels.volume }}"
```

- network_sent#

```
groups:
  - name: windows_exporter
    rules:
    - alert: network_sent(Windows exporter)
```

```
      expr: 100 < rate(windows_net_packets_sent_total[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0405"
        jp1_pc_metricname: "windows_net_packets_sent_total"
      annotations:
        jp1_pc_firing_description: "The network transmission speed exceede
d the threshold (100 packets per second).value={{ $value }}Packets/sec, ni
c={{ $labels.nic }}"
        jp1_pc_resolved_description: "The network transmission speed has d
ropped below the threshold (100 packets per second).nic={{ $labels.nic }}"
```

- network_received#

```
groups:
  - name: windows_exporter
    rules:
    - alert: network_received(Windows exporter)
      expr: 100 < rate(windows_net_packets_received_total[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0406"
        jp1_pc_metricname: "windows_net_packets_received_total"
      annotations:
        jp1_pc_firing_description: "The network receive speed exceeded th
e threshold (100 packets per second).value={{ $value }}Packets/sec, nic={
{ $labels.nic }}"
        jp1_pc_resolved_description: "The network receive speed has droppe
d below the threshold (100 packets per second).nic={{ $labels.nic }}"
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "`groups:`" or duplicate `name` with the same group-name.

■Metric alert definition example in *Windows exporter (process monitoring) metric definition file*

- process_pgm_process_count#

```
groups:
 - name: windows_exporter
  rules:
   - alert: process_pgm_process_count(Windows exporter)
     expr: absent(windows_process_start_time{instance="integrated-agent-ho
st-name:Windows-exporter-port-number", job="jpc_windows", jp1_pc_exporter=
"JPC Windows exporter", jp1_pc_nodelabel="monitored-process-name",process=
"monitored-process-name"}) == 1
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0414"
        jp1_pc_metricname: "windows_process_start_time"
      annotations:
        jp1_pc_firing_description: "The number of processes has fallen bel
ow the threshold (1 process)."
        jp1_pc_resolved_description: "The number of processes has exceede
d the threshold (1 process)."
```

#

This uses a threshold value of 1 as an example. Change this value based on the number of monitoring targets.

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate.

- Alert definition example for metrics in "Windows exporter (Service monitoring) metric definition file"

- service_state#

```
groups:
  - name: windows_exporter
    rules:
    - alert: service_state(Windows exporter)
      expr: windows_service_state{state="running"} == 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0420"
        jp1_pc_metricname: "windows_service_state"
      annotations:
        jp1_pc_firing_description: "The status of the serviceis not runnin
g."
        jp1_pc_resolved_description: "The service status is now running."
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "groups:" or duplicate name with the same group-name.

- Alert definition example for metrics in "Node exporter for AIX metric definition file"

- cpu_used_rate#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: cpu_used_rate(Node exporter for AIX)
      expr: 80 < ((avg by(instance,job,jp1_pc_nodelabel,jp1_pc_exporter) (
rate(node_cpu{mode="sys"}[2m])))+(avg by(instance,job,jp1_pc_nodelabel,jp1
_pc_exporter) ((rate(node_cpu{mode="user"}[2m])))))*100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0901"
        jp1_pc_metricname: "node_cpu"
      annotations:
        jp1_pc_firing_description: "CPU utilization has exceeded threshol
```

```
d (80%).value={{ $value }}%"
        jp1_pc_resolved_description: "CPU utilization has fallen below th
e threshold (80%)."
```

- memory_unused#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: memory_unused(Node exporter for AIX)
      expr: 1 > aix_memory_real_avail/1024/1024/1024*4096
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0902"
        jp1_pc_metricname: "aix_memory_real_avail"
      annotations:
        jp1_pc_firing_description: "Free memory falls below threshold (1 g
igabyte). value={{ $value }}gigabyte"
        jp1_pc_resolved_description: "The amount of free memory has exceed
ed the threshold value (1 gigabyte)."
```

- memory_unused_rate#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: memory_unused_rate(Node exporter for AIX)
      expr: aix_memory_real_avail / aix_memory_real_total * 100 < 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0902"
        jp1_pc_metricname: "aix_memory_real_avail,aix_memory_real_total"
      annotations:
        jp1_pc_firing_description: "Free-memory percentage dropped below t
hreshold (10%). value={{ $value }}%"
        jp1_pc_resolved_description: "Free-memory percentage exceeded thre
shold (10%)."
```

- disk_unused#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_unused(Node exporter for AIX))
      expr: 10 > node_filesystem_free_bytes{job="jpc_node_aix"}/(1024*1024
*1024)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0903"
        jp1_pc_metricname: "node_filesystem_free_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk space dropped below threshol
d (10 gigabytes). value={{ $value }}gigabytes, mountpoint={{ $labels.mount
point }}"
        jp1_pc_resolved_description: "Free disk space exceeds threshold (1
0 gigabytes). mountpoint={{ $labels.mountpoint }}"
```

Note

If you want to monitor both Node exporter and Node exporter for AIX on a single Prometheus, specify `job` labels in `expr` of `disk_unused` in Node exporter alert-definition to distinguish between metric for Node exporter and Node exporter for AIX. For more information, see `disk_unused` in "Metric alert definition example in *Node exporter metric definition file*" above.

- disk_unused_rate[#]

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_unused_rate(Node exporter for AIX)
      expr: node_filesystem_free_bytes{job="jpc_node_aix"} / node_filesyst
em_size_bytes{job="jpc_node_aix"} * 100 < 10
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0903"
        jp1_pc_metricname: "node_filesystem_free_bytes,node_filesystem_siz
e_bytes"
      annotations:
        jp1_pc_firing_description: "Free disk percentage dropped below thr
eshold (10%). value={{ $value }}%, mountpoint={{ $labels.mountpoint }}"
        jp1_pc_resolved_description: "Free disk percentage exceeds thresho
ld (10%). mountpoint={{ $labels.mountpoint }}"
```

Note

If you want to monitor both Node exporter and Node exporter for AIX on a single Prometheus, specify `job` labels in `expr` of `disk_unused_rate` in Node exporter alert-definition to distinguish between metric for Node exporter and Node exporter for AIX. For details, see `disk_unused_rate` in "Metric alert definition example in *Node exporter metric definition file*" above.

- disk_busy_rate[#]

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_busy_rate(Node exporter for AIX)
      expr: 70 < rate(aix_disk_time[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0904"
        jp1_pc_metricname: "aix_disk_time"
      annotations:
        jp1_pc_firing_description: "Disk busy rate exceeded threshold (70%
). value={{ $value }}%, device={{ $labels.device }}"
        jp1_pc_resolved_description: "Disk busy rate dropped below thresho
ld (70%). device={{ $labels.device }}"
```

- disk_read_latency#

```
ggroups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_read_latency(Node exporter for AIX)
      expr: rate(aix_disk_rserv[2m]) / rate(aix_disk_xrate[2m])/1000/1000/
1000 > 0.1 and rate(aix_disk_xrate[2m]) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0904"
        jp1_pc_metricname: "aix_disk_rserv,aix_disk_xrate"
      annotations:
        jp1_pc_firing_description: "Disk read latency exceeds threshold (0
.1 sec.), value={{ $value }}sec., device={{ $labels.device }}"
        jp1_pc_resolved_description: "Disk read latency dropped below thre
shold (0.1 sec). device={{ $labels.device }}"
```

- disk_write_latency#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_write_latency(Node exporter for AIX)
      expr: rate(aix_disk_wserv[2m]) / (rate(aix_disk_xfers[2m]) - rate(ai
x_disk_xrate[2m]))/1000/1000/1000 > 0.1 and (rate(aix_disk_xfers[2m]) - ra
te(aix_disk_xrate[2m])) > 0
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0904"
        jp1_pc_metricname: "aix_disk_wserv,aix_disk_xfers,aix_disk_xrate"
      annotations:
        jp1_pc_firing_description: "Disc write latency exceeds threshold (
0.1 sec.), value={{ $value }}sec., device={{ $labels.device }}"
        jp1_pc_resolved_description: "Disc write latency dropped below thr
eshold (0.1 sec.). device={{ $labels.device }}"
```

- disk_io_latency#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: disk_io_latency(Node exporter for AIX)
      expr: (rate(aix_disk_rserv[2m]) + rate(aix_disk_wserv[2m])) / rate(a
ix_disk_xfers[2m])/1000/1000/1000 > 0.1 and (rate(aix_disk_xfers[2m]) > 0)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0904"
        jp1_pc_metricname: "aix_disk_wserv,aix_disk_rserv,aix_disk_xfers"
      annotations:
        jp1_pc_firing_description: "Disk IO latency exceeded threshold (0.
1 sec.), value={{ $value }}sec., device={{ $labels.device }}"
        jp1_pc_resolved_description: "Disc IO latency dropped below thresh
old (0.1 sec.). device={{ $labels.device }}"
```

- network_sent#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: network_sent(Node exporter for AIX)
      expr: 100 < rate(aix_netinterface_opackets[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0905"
        jp1_pc_metricname: "aix_netinterface_opackets"
      annotations:
        jp1_pc_firing_description: "Network sending rate exceeds threshol
d (100 packets/sec.), value={{ $value }}packets/sec, device={{ $labels.dev
ice }}"
        jp1_pc_resolved_description: "Network sending rate dropped below t
hreshold (100 packets/sec). device={{ $labels.device }}"
```

- network_received#

```
groups:
  - name: node_exporter_AIX
    rules:
    - alert: network_received(Node exporter for AIX)
      expr: 100 < rate(aix_netinterface_ipackets[2m])
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0905"
        jp1_pc_metricname: "aix_netinterface_ipackets"
      annotations:
        jp1_pc_firing_description: "Network-Receive Rate Exceeded Threshol
d (100 Packets/sec.) value={{ $value }}Packets/sec., device={{ $labels.dev
ice }}"
        jp1_pc_resolved_description: "Network receive rate dropped below t
hreshold (100 packets/sec). device={{ $labels.device }}"
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "groups:" or duplicate name with the same group-name.

■Metric alert definition example in *Blackbox exporter metric definition file*

- probe_success#

```
groups:
  - name: blackbox_exporter
    rules:
    - alert: probe_success(Blackbox exporter)
      expr: 0 == probe_success
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0501"
        jp1_pc_metricname: "probe_success"
      annotations:
        jp1_pc_firing_description: "通信に失敗しました。value={{ $value }}"
        jp1_pc_resolved_description: "通信に成功しました。"
```

- probe_duration_seconds#

```
groups:
  - name: blackbox_exporter
    rules:
    - alert: probe_duration_seconds(Blackbox exporter)
      expr: 5 < probe_duration_seconds
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0502"
        jp1_pc_metricname: "probe_duration_seconds"
      annotations:
        jp1_pc_firing_description: "プローブ期間がしきい値(5秒)を上回りました。va
lue={{ $value }}秒"
        jp1_pc_resolved_description: "プローブ期間がしきい値(5秒)を下回りま
した。"
```

- probe_icmp_duration_seconds#

```
groups:
  - name: blackbox_exporter
    rules:
    - alert: probe_icmp_duration_seconds(Blackbox exporter)
      expr: 3 < probe_icmp_duration_seconds
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0503"
        jp1_pc_metricname: "probe_icmp_duration_seconds"
      annotations:
        jp1_pc_firing_description: "ICMP期間がしきい値(3秒)を上回りました。valu
e={{ $value }}秒, phase={{ $labels.phase }}"
        jp1_pc_resolved_description: "ICMP期間がしきい値(3秒)を下回りました。"
```

- probe_http_duration_seconds#

```
groups:
  - name: blackbox_exporter
    rules:
    - alert: probe_http_duration_seconds(Blackbox exporter)
      expr: 3 < probe_http_duration_seconds
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0504"
        jp1_pc_metricname: "probe_http_duration_seconds"
      annotations:
        jp1_pc_firing_description: "HTTPリクエスト期間がしきい値(3秒)を上回りま
した。value={{ $value }}秒, phase={{ $labels.phase }}"
        jp1_pc_resolved_description: "HTTPリクエスト期間がしきい値(3秒)を下回り
ました。"
```

- probe_http_status_code#

```
groups:
  - name: blackbox_exporter
    rules:
    - alert: probe_http_status_code(Blackbox exporter)
      expr: 200 != probe_http_status_code
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0505"
        jp1_pc_metricname: "probe_http_status_code"
      annotations:
        jp1_pc_firing_description: "HTTPステータスが200ではありません。value={
{ $value }}"
        jp1_pc_resolved_description: "HTTPステータスが200になりました。"
```

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "`groups:`" or duplicate `name` with the same group-name.

■Metric alert definition example in *Yet another cloudwatch exporter metric definition file*

- aws_ec2_cpuutilization_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_ec2_cpuutilization_average(Yet another cloudwatch exporte
r)
      expr: 80 < aws_ec2_cpuutilization_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0601"
        jp1_pc_metricname: "aws_ec2_cpuutilization_average"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%)."
```

- aws_ec2_disk_read_bytes_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_ec2_disk_read_bytes_sum(Yet another cloudwatch exporter)
      expr: 10240 < aws_ec2_disk_read_bytes_sum / 1024
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0602"
        jp1_pc_metricname: "aws_ec2_disk_read_bytes_sum"
      annotations:
        jp1_pc_firing_description: "インスタンスストアボリュームの読み取りキロバイ
ト数がしきい値(10,240KB)を上回りました。value={{ $value }}KB"
        jp1_pc_resolved_description: "インスタンスストアボリュームの読み取りキロ
バイト数がしきい値(10,240KB)を下回りました。"
```

- aws_ec2_disk_write_bytes_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_ec2_disk_write_bytes_sum(Yet another cloudwatch exporter)
      expr: 10240 < aws_ec2_disk_write_bytes_sum / 1024
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0603"
        jp1_pc_metricname: "aws_ec2_disk_write_bytes_sum"
      annotations:
        jp1_pc_firing_description: "インスタンスストアボリュームの書き込みキロバイ
ト数がしきい値(10,240KB)を上回りました。value={{ $value }}KB"
        jp1_pc_resolved_description: "インスタンスストアボリュームの書き込みキロ
バイト数がしきい値(10,240KB)を下回りました。"
```

- aws_lambda_errors_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_lambda_errors_sum(Yet another cloudwatch exporter)
      expr: 0 < aws_lambda_errors_sum{dimension_Resource=""}
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0604"
        jp1_pc_metricname: "aws_lambda_errors_sum"
      annotations:
        jp1_pc_firing_description: "関数エラーが発生した呼び出しの数がしきい値(0
個)を上回りました。value={{ $value }}個"
        jp1_pc_resolved_description: "関数エラーが発生した呼び出しの数がしきい値(
0個)を下回りました。"
```

- aws_lambda_duration_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_lambda_duration_average(Yet another cloudwatch exporter)
      expr: 5000 < aws_lambda_duration_average{dimension_Resource=""}
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0605"
        jp1_pc_metricname: "aws_lambda_duration_average"
      annotations:
        jp1_pc_firing_description: "関数コードがイベントの処理に費やす時間がしきい
値(5000ミリ秒)を上回りました。value={{ $value }}ミリ秒"
        jp1_pc_resolved_description: "関数コードがイベントの処理に費やす時間がし
きい値(5000ミリ秒)を下回りました。"
```

- aws_s3_bucket_size_bytes_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_s3_bucket_size_bytes_sum(Yet another cloudwatch exporter)
      expr: 1024 < aws_s3_bucket_size_bytes_sum / (1024*1024*1024)
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0606"
        jp1_pc_metricname: "aws_s3_bucket_size_bytes_sum"
      annotations:
        jp1_pc_firing_description: "バケットの保存データ量がしきい値(1024GB)を上
回りました。value={{ $value }}GB"
        jp1_pc_resolved_description: "バケットの保存データ量がしきい値(1024GB)を
下回りました。"
```

- aws_s3_5xx_errors_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_s3_5xx_errors_sum(Yet another cloudwatch exporter)
      expr: 0 < aws_s3_5xx_errors_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0607"
        jp1_pc_metricname: "aws_s3_5xx_errors_sum"
      annotations:
        jp1_pc_firing_description: "バケットへのリクエストに対して，HTTP 5xx
サーバーエラーステータスコードを返却される数が，しきい値(0個)を上回りました。value={{
$value }}個"
        jp1_pc_resolved_description: "バケットへのリクエストに対して，HTTP 5xx
サーバーエラーステータスコードを返却される数が，しきい値(0個)を下回りました。"
```

- aws_dynamodb_consumed_read_capacity_units_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_dynamodb_consumed_read_capacity_units_sum(Yet another clo
udwatch exporter)
      expr: 600 < aws_dynamodb_consumed_read_capacity_units_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0608"
        jp1_pc_metricname: "aws_dynamodb_consumed_read_capacity_units_sum"
      annotations:
        jp1_pc_firing_description: "消費された読み込み容量ユニットの合計数がしきい
値(600個)を上回りました。value={{ $value }}個"
        jp1_pc_resolved_description: "消費された読み込み容量ユニットの合計数がし
きい値(600個)を下回りました。"
```

- aws_dynamodb_consumed_write_capacity_units_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_dynamodb_consumed_write_capacity_units_sum(Yet another cl
oudwatch exporter)
      expr: 600 < aws_dynamodb_consumed_write_capacity_units_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0609"
        jp1_pc_metricname: "aws_dynamodb_consumed_write_capacity_units_su
m"
      annotations:
        jp1_pc_firing_description: "消費された書き込み容量ユニットの合計数がしきい
値(600個)を上回りました。value={{ $value }}個"
        jp1_pc_resolved_description: "消費された書き込み容量ユニットの合計数がし
きい値(600個)を下回りました。"
```

- aws_states_execution_time_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_states_execution_time_average(Yet another cloudwatch expo
rter)
      expr: 5000 < aws_states_execution_time_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0610"
        jp1_pc_metricname: "aws_states_execution_time_average"
      annotations:
        jp1_pc_firing_description: "Step Functionsの実行時間がしきい値(5000ミ
リ秒)を上回りました。value={{ $value }}ミリ秒"
        jp1_pc_resolved_description: "Step Functionsの実行時間がしきい値(5000
ミリ秒)を下回りました。"
```

- aws_states_executions_failed_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_states_executions_failed_sum(Yet another cloudwatch expor
ter)
      expr: 0 < aws_states_executions_failed_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0611"
        jp1_pc_metricname: "aws_states_executions_failed_sum"
      annotations:
        jp1_pc_firing_description: "Step Functionsの実行失敗数がしきい値(0個)
を上回りました。value={{ $value }}個"
        jp1_pc_resolved_description: "Step Functionsの実行失敗数がしきい値(0
個)を下回りました。"
```

- aws_sqs_approximate_number_of_messages_delayed_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_sqs_approximate_number_of_messages_delayed_sum(Yet anothe
r cloudwatch exporter)
      expr: 0 < aws_sqs_approximate_number_of_messages_delayed_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0612"
        jp1_pc_metricname: "aws_sqs_approximate_number_of_messages_delayed
_sum"
      annotations:
        jp1_pc_firing_description: "遅延キューメッセージ数がしきい値(0個)を上回り
```

```
ました。value={{ $value }}個"
        jp1_pc_resolved_description: "遅延キューメッセージ数がしきい値(0個)を下回
りました。"
```

- aws_sqs_number_of_messages_deleted_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_sqs_number_of_messages_deleted_sum(Yet another cloudwatc
h exporter)
      expr:  0 < aws_sqs_number_of_messages_deleted_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0613"
        jp1_pc_metricname: "aws_sqs_number_of_messages_deleted_sum"
      annotations:
        jp1_pc_firing_description: "削除キューメッセージ数がしきい値(0個)を上回り
ました。value={{ $value }}個"
        jp1_pc_resolved_description: "削除キューメッセージ数がしきい値(0個)を下回
りました。"
```

- aws_ecs_cpuutilization_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_ecs_cpuutilization_average(Yet another cloudwatch exporte
r)
      expr: 80 < aws_ecs_cpuutilization_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0614"
        jp1_pc_metricname: "aws_ecs_cpuutilization_average"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%)."
```

- aws_ecs_memory_utilization_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_ecs_memory_utilization_average(Yet another cloudwatch exp
orter)
      expr: 80 < aws_ecs_memory_utilization_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0615"
        jp1_pc_metricname: "aws_ecs_memory_utilization_average"
      annotations:
        jp1_pc_firing_description: "Memory usage has exceeded the threshol
d (80%). value={{ $value }}%"
        jp1_pc_resolved_description: "Memory usage has fallen below the th
reshold (80%)."
```

- aws_rds_cpuutilization_average#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_rds_cpuutilization_average(Yet another cloudwatch exporte
r)
      expr: 80 < aws_rds_cpuutilization_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0616"
        jp1_pc_metricname: "aws_rds_cpuutilization_average"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%)."
```

- aws_sns_number_of_notifications_failed_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_sns_number_of_notifications_failed_sum(Yet another cloudw
atch exporter)
      expr: 0 < aws_sns_number_of_notifications_failed_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0617"
        jp1_pc_metricname: "aws_sns_number_of_notifications_failed_sum"
      annotations:
        jp1_pc_firing_description: "The number of rejected messages has ex
ceeded the threshold (0 messages). value={{ $value }} messages"
        jp1_pc_resolved_description: "The number of rejected messages has
fallen below the threshold (0 messages)."
```

- aws_sns_number_of_notifications_filtered_out_sum#

```
groups:
  - name: yet_another_cloudwatch_exporter
    rules:
    - alert: aws_sns_number_of_notifications_filtered_out_sum(Yet another
cloudwatch exporter)
      expr: 0 < aws_sns_number_of_notifications_filtered_out_sum
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0618"
        jp1_pc_metricname: "aws_sns_number_of_notifications_filtered_out_s
um"
      annotations:
        jp1_pc_firing_description: "The number of rejected messages has ex
ceeded the threshold (0 messages). value={{ $value }} messages"
        jp1_pc_resolved_description: "The number of rejected messages has
fallen below the threshold (0 messages)."
```

#

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate.

■Metric alert definition example in *Promitor metric definition file*

- azure_virtual_machine_disk_read_bytes_total#

```
groups:
  - name: promitor
    rules:
    - alert: azure_virtual_machine_disk_read_bytes_total(Promitor)
      expr: 10485760 < azure_virtual_machine_disk_read_bytes_total
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0901"
        jp1_pc_metricname: "azure_virtual_machine_disk_read_bytes_total"
      annotations:
        jp1_pc_firing_description: "The number of disk read bytes has exce
eded the threshold (10485760 bytes). value={{ $value }} bytes"
        jp1_pc_resolved_description: "The number of disk read bytes has fa
llen below the threshold (10485760 bytes)."
```

- azure_virtual_machine_disk_write_bytes_total#

```
groups:
  - name: promitor
    rules:
    - alert: azure_virtual_machine_disk_write_bytes_total(Promitor)
      expr: 10485760 < azure_virtual_machine_disk_write_bytes_total
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0902"
        jp1_pc_metricname: "azure_virtual_machine_disk_write_bytes_total"
      annotations:
        jp1_pc_firing_description: "The number of disk write bytes has exc
eeded the threshold (10485760 bytes). value={{ $value }} bytes"
        jp1_pc_resolved_description: "The number of disk write bytes has f
allen below the threshold (10485760 bytes)."
```

- azure_virtual_machine_percentage_cpu_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_virtual_machine_percentage_cpu_average(Promitor)
      expr: 80 < azure_virtual_machine_percentage_cpu_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0903"
        jp1_pc_metricname: "azure_virtual_machine_percentage_cpu_average"
      annotations:
        jp1_pc_firing_description: "The percentage of allocated compute un
its has exceeded the threshold (80%). value={{ $value }}%"
        jp1_pc_resolved_description: "The percentage of allocated compute
units has fallen below the threshold (80%)."
```

- azure_blob_storage_availability_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_blob_storage_availability_average(Promitor)
      expr: 100 > azure_blob_storage_availability_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0904"
        jp1_pc_metricname: "azure_blob_storage_availability_average"
      annotations:
        jp1_pc_firing_description: "The percentage of availability has fal
len below the threshold (100%). value={{ $value }}%"
        jp1_pc_resolved_description: "The percentage of availability has e
xceeded the threshold (100%)."
```

- azure_blob_storage_blob_capacity_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_blob_storage_blob_capacity_average(Promitor)
      expr: 1099511627776 < azure_blob_storage_blob_capacity_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0905"
        jp1_pc_metricname: "azure_blob_storage_blob_capacity_average"
      annotations:
        jp1_pc_firing_description: "The storage capacity has exceeded the
threshold (1099511627776 bytes). value={{ $value }} bytes"
        jp1_pc_resolved_description: "The storage capacity has fallen belo
w the threshold (1099511627776 bytes)."
```

- azure_function_app_http5xx_total#

```
groups:
  - name: promitor
    rules:
    - alert: azure_function_app_http5xx_total(Promitor)
      expr: 0 < azure_function_app_http5xx_total
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0906"
        jp1_pc_metricname: "azure_function_app_http5xx_total"
      annotations:
        jp1_pc_firing_description: "The number of 5xx server errors has ex
ceeded the threshold (0 errors). value={{ $value }} errors"
        jp1_pc_resolved_description: "The number of 5xx server errors has
fallen below the threshold (0 errors)."
```

- azure_function_app_http_response_time_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_function_app_http_response_time_average(Promitor)
      expr: 0 < azure_function_app_http_response_time_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0907"
        jp1_pc_metricname: "azure_function_app_http_response_time_average"
      annotations:
        jp1_pc_firing_description: "The response time has exceeded the thr
eshold (5 seconds). value={{ $value }} seconds"
        jp1_pc_resolved_description: "The response time has fallen below t
he threshold (5 seconds)."
```

- azure_cosmos_db_total_request_units_total#

```
groups:
  - name: promitor
    rules:
    - alert: azure_cosmos_db_total_request_units_total(Promitor)
      expr: 600 < azure_cosmos_db_total_request_units_total
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0908"
        jp1_pc_metricname: "azure_cosmos_db_total_request_units_total"
      annotations:
        jp1_pc_firing_description: "The number of consumed request units h
as exceeded the threshold (600 units). value={{ $value }} units, collectio
nname={{ $labels.collectionname }}"
```

```
        jp1_pc_resolved_description: "The number of consumed request unit
s has fallen below the threshold (600 units). collectionname={{ $labels.co
llectionname }}"
```

- azure_logic_app_runs_failed_total#

```
groups:
  - name: promitor
    rules:
    - alert: azure_logic_app_runs_failed_total(Promitor)
      expr: 0 < azure_logic_app_runs_failed_total
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0910"
        jp1_pc_metricname: "azure_logic_app_runs_failed_total"
      annotations:
        jp1_pc_firing_description: "The number of workflow errors has exce
eded the threshold (0 errors). value={{ $value }} errors"
        jp1_pc_resolved_description: "The number of workflow errors has fa
llen below the threshold (0 errors)."
```

- azure_container_instance_cpu_usage_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_container_instance_cpu_usage_average(Promitor)
      expr: 800 < azure_container_instance_cpu_usage_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0911"
        jp1_pc_firing_description: "CPU usage (millicores) has exceeded th
e threshold (800 millicores). value={{ $value }} millicores"
        jp1_pc_resolved_description: "CPU usage (millicores) has fallen be
low the threshold (800 millicores)."
```

- azure_kubernetes_service_kube_pod_status_phase_average_failed#

```
groups:
  - name: promitor
    rules:
    - alert: azure_kubernetes_service_kube_pod_status_phase_average_failed
(Promitor)
      expr: 0 < azure_kubernetes_service_kube_pod_status_phase_average_fai
led
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0912"
        jp1_pc_metricname: "azure_kubernetes_service_kube_pod_status_phase
```

```
_average_failed"
      annotations:
        jp1_pc_firing_description: "The number of failed pods has exceede
d the threshold (0 pods). value={{ $value }} pods"
        jp1_pc_resolved_description: "The number of failed pods has falle
n below the threshold (0 pods)."
```

- azure_kubernetes_service_kube_pod_status_phase_average_pending#

```
groups:
  - name: promitor
    rules:
    - alert: azure_kubernetes_service_kube_pod_status_phase_average_pendin
g(Promitor)
      expr: 0 < azure_kubernetes_service_kube_pod_status_phase_average_pen
ding
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0913"
        jp1_pc_metricname: "azure_kubernetes_service_kube_pod_status_phase
_average_pending"
      annotations:
        jp1_pc_firing_description: "The number of pending pods has exceede
d the threshold (0 pods). value={{ $value }} pods"
        jp1_pc_resolved_description: "The number of pending pods has falle
n below the threshold (0 pods)."
```

- azure_kubernetes_service_kube_pod_status_phase_average_unknown#

```
groups:
  - name: promitor
    rules:
    - alert: azure_kubernetes_service_kube_pod_status_phase_average_unknow
n(Promitor)
      expr: 0 < azure_kubernetes_service_kube_pod_status_phase_average_unk
nown
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0914"
        jp1_pc_metricname: "azure_kubernetes_service_kube_pod_status_phase
_average_unknown"
      annotations:
        jp1_pc_firing_description: "The number of unknown pods has exceede
d the threshold (0 pods). value={{ $value }} pods"
        jp1_pc_resolved_description: "The number of unknown pods has falle
n below the threshold (0 pods)."
```

- azure_file_storage_availability_average#

```
groups:
  - name: promitor
    rules:
```

```
    - alert: azure_file_storage_availability_average(Promitor)
      expr: 100 > azure_file_storage_availability_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0915"
        jp1_pc_metricname: "azure_file_storage_availability_average"
      annotations:
        jp1_pc_firing_description: "The percentage of availability has fal
len below the threshold (100%). value={{ $value }}%, fileshare={{ $labels.
fileshare }}"
        jp1_pc_resolved_description: "The percentage of availability has e
xceeded the threshold (100%). fileshare={{ $labels.fileshare }}"
```

- azure_service_bus_namespace_deadlettered_messages_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_service_bus_namespace_deadlettered_messages_average(Pro
mitor)
      expr: 0 < azure_service_bus_namespace_deadlettered_messages_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0916"
        jp1_pc_metricname: "azure_service_bus_namespace_deadlettered_messa
ges_average"
      annotations:
        jp1_pc_firing_description: "The number of dead-lettered messages h
as exceeded the threshold (0 messages). value={{ $value }} messages, entit
y_name={{ $labels.entity_name }}"
        jp1_pc_resolved_description: "The number of dead-lettered message
s has fallen below the threshold (0 messages). entity_name={{ $labels.enti
ty_name }}"
```

- azure_sql_database_cpu_percent_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_sql_database_cpu_percent_average(Promitor)
      expr: 80 < azure_sql_database_cpu_percent_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0917"
        jp1_pc_metricname: "azure_sql_database_cpu_percent_average"
      annotations:
        jp1_pc_firing_description: "CPU percentage has exceeded the thresh
old (80%). value={{ $value }}%, server={{ $labels.server }}"
```

```
        jp1_pc_resolved_description: "CPU percentage has fallen below the
threshold (80%). server={{ $labels.server }}"
```

- azure_sql_elastic_pool_cpu_percent_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_sql_elastic_pool_cpu_percent_average(Promitor)
      expr: 80 < azure_sql_elastic_pool_cpu_percent_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0920"
        jp1_pc_metricname: "azure_sql_elastic_pool_cpu_percent_average"
      annotations:
        jp1_pc_firing_description: "CPU percentage has exceeded the thresh
old (80%). value={{ $value }}%, server={{ $labels.server }}"
        jp1_pc_resolved_description: "CPU percentage has fallen below the
threshold (80%). server={{ $labels.server }}"
```

- azure_sql_managed_instance_avg_cpu_percent_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_sql_managed_instance_avg_cpu_percent_average(Promitor)
      expr: 80 < azure_sql_managed_instance_avg_cpu_percent_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0922"
        jp1_pc_metricname: "azure_sql_managed_instance_avg_cpu_percent_ave
rage"
      annotations:
        jp1_pc_firing_description: "Average CPU percentage has exceeded th
e threshold (80%). value={{ $value }}%"
        jp1_pc_resolved_description: "Average CPU percentage has fallen be
low the threshold (80%)."
```

- azure_sql_managed_instance_io_bytes_read_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_sql_managed_instance_io_bytes_read_average(Promitor)
      expr: 10485760 < azure_sql_managed_instance_io_bytes_read_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0923"
        jp1_pc_metricname: "azure_sql_managed_instance_io_bytes_read_avera
```

```
ge"
      annotations:
        jp1_pc_firing_description: "The number of IO bytes read has exceed
ed the threshold (10485760 bytes). value={{ $value }} bytes"
        jp1_pc_resolved_description: "The number of disk read bytes has fa
llen below the threshold (10485760 bytes)."
```

- azure_sql_managed_instance_io_bytes_written_average#

```
groups:
  - name: promitor
    rules:
    - alert: azure_sql_managed_instance_io_bytes_written_average(Promitor)
      expr: 10485760 < azure_sql_managed_instance_io_bytes_written_average
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/AZURE/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0924"
        jp1_pc_metricname: "azure_sql_managed_instance_io_bytes_written_av
erage"
      annotations:
        jp1_pc_firing_description: "The number of IO bytes written has exc
eeded the threshold (10485760 bytes). value={{ $value }} bytes"
        jp1_pc_resolved_description: "The number of IO bytes written has f
allen below the threshold (10485760 bytes)."
```

#

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate.

■Metric alert definition example in *Script exporter metric definition file*

- azure_virtual_machine_disk_read_bytes_total#1

```
groups:
  - name: script_exporter
    rules:
    - alert: script_success(Script exporter)
      expr: 0 == script_success
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1401"
        jp1_pc_metricname: "script_success"
      annotations:
        jp1_pc_firing_description: "Failed to execute script. value={{ $va
lue }}"
        jp1_pc_resolved_description: "Script successfully executed."
```

- script_duration_seconds#1, #2

```
groups:
  - name: script_exporter
    rules:
```

```
    - alert: script_duration_seconds(Script exporter)
      expr: 60 < script_duration_seconds
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1402"
        jp1_pc_metricname: "script_duration_seconds"
      annotations:
        jp1_pc_firing_description: "The script execution time has exceede
d the threshold (60 seconds). value={{ $value }} seconds"
        jp1_pc_resolved_description: "The script execution time has falle
n below the threshold (60 seconds)."
```

- script_exit_code#1

```
groups:
  - name: script_exporter
    rules:
    - alert: script_exit_code(Script exporter)
      expr: 0 != script_exit_code
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1403"
        jp1_pc_metricname: "script_exit_code"
      annotations:
        jp1_pc_firing_description: "Failed to execute script. value={{ $va
lue }}"
        jp1_pc_resolved_description: "Script successfully executed."
```

#1

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate.

#2

This uses a threshold value of 60 as an example. Change this value based on the number of monitoring targets.

- Alert definition example for metrics in "OracleDB exporter metric definition file"

- oracledb_up#

```
groups:
  - name: oracledb_exporter
    rules:
    - alert: oracledb_down(OracleDB exporter)
      expr: oracledb_up != 1
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0801"
        jp1_pc_metricname: "oracledb_up"
      annotations:
        jp1_pc_firing_description: "OracleDB stopped.instance={{ $labels.i
nstance }}"
        jp1_pc_resolved_description: "OracleDB started. instance={{ $label
s.instance }}"
```

- cache_hit_ratio_percent#

```
groups:
  - name: oracledb_exporter
    rules:
    - alert: cache_hit_ratio_percentage_under_60(OracleDB exporter)
      expr: (1 - (rate(oracledb_activity_physical_reads_cache[2m]) / (rate
(oracledb_activity_consistent_gets_from_cache[2m])+rate(oracledb_activity_
db_block_gets_from_cache[2m]))))*100  < 60
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0802"
        jp1_pc_metricname: "oracledb_activity_physical_reads_cache,oracled
b_activity_consistent_gets_from_cache,oracledb_activity_db_block_gets_from
_cache"
      annotations:
        jp1_pc_firing_description: "Cache hit rate for OracleDB dropped be
low 60%. instance={{ $labels.instance }}, value={{ $value }}"
        jp1_pc_resolved_description: "OracleDB cache hit rate is now over
60%. instance={{ $labels.instance }}"
```

- tablespace_used_percent#

```
groups:
  - name: oracledb_exporter
    rules:
    - alert: oracledb_tablespace_used_percent_over_90(OracleDB exporter)
      expr: oracledb_tablespace_used_percent > 90
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0803"
        jp1_pc_metricname: "oracledb_tablespace_used_percent"
      annotations:
        jp1_pc_firing_description: "Tablespace usage for OracleDB exceede
d 90%. instance={{ $labels.instance }}, value={{ $value }}"
        jp1_pc_resolved_description: "Tablespace usage for OracleDB is 90
% or less. instance={{ $labels.instance }}"
```

- execute_count#

```
groups:
  - name: oracledb_exporter
    rules:
    - alert: oracledb_activity_execute_count_over_1000(OracleDB exporter)
      expr: rate(oracledb_activity_execute_count[2m])*60 > 1000
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "0804"
        jp1_pc_metricname: "oracledb_activity_execute_count"
      annotations:
        jp1_pc_firing_description: "SQL statement executed more than 1000
times. instance={{ $labels.instance }}, value={{ $value }}"
        jp1_pc_resolved_description: "The number of executions of SQL stat
ement is less than 1000. instance={{ $labels.instance }}"
```

- parse_count#

  Please see the execute_count to create it.

- user_commit_count#

  Please see the execute_count to create it.

- user_rollback_count#

  Please see the execute_count to create it.

- resource_used#

  Please see the tablespace_used_percent to create it.

- session_count#

  Please see the tablespace_used_percent to create it.

#

If you define more than one alert in the same monitoring agent host, be careful not to specify duplicate "groups:" or duplicate name with the same group-name.

■Metric alert definition example in *Container monitoring metric definition file*

- kube_job_status_failed#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_job_status_failed(Kube state metrics)
     expr: 0 < kube_job_status_failed * on(job_name, namespace) group_left
() kube_job_owner{owner_kind="<none>", owner_name="<none>"}
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1201"
        jp1_pc_metricname: "kube_job_status_failed, kube_job_owner"
        jp1_pc_nodelabel: "{{ $labels.namespace }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of failed pods has exceede
d the threshold (0 pods). value={{ $value }} pods, job_name={{ $labels.job
_name }}"
        jp1_pc_resolved_description: "The number of failed pods has falle
n below the threshold (0 pods). job_name={{ $labels.job_name }}"
```

- kube_pod_status_pending#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_pod_status_pending(Kube state metrics)
     expr: 0 < sum by (pod, namespace, instance, job) (kube_pod_status_pha
se{phase="Pending"})
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1202"
        jp1_pc_metricname: "kube_pod_status_pending"
        jp1_pc_nodelabel: "{{ $labels.namespace }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of pending pods has exceede
d the threshold (0 pods). value={{ $value }} pods, pod={{ $labels.pod }}"
        jp1_pc_resolved_description: "The number of pending pods has falle
n below the threshold (0 pods). pod={{ $labels.pod }}"
```

- kube_pod_status_failed#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_pod_status_failed(Kube state metrics)
     expr: 0 < sum by (pod, namespace, instance, job) (kube_pod_status_pha
se{phase="Failed"}
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1203"
        jp1_pc_metricname: "kube_pod_status_phase"
        jp1_pc_nodelabel: "{{ $labels.namespace }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of failed pods has exceede
d the threshold (0 pods). value={{ $value }} pods, pod={{ $labels.pod }}"
        jp1_pc_resolved_description: "The number of failed pods has falle
n below the threshold (0 pods). pod={{ $labels.pod }}"
```

- kube_pod_status_unknown#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_pod_status_unknown(Kube state metrics)
     expr: 0 < sum by (pod, namespace, instance) (kube_pod_status_phase{ph
ase="Unknown"}
```

```
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1204"
        jp1_pc_metricname: "kube_pod_status_phase"
        jp1_pc_nodelabel: "{{ $labels.namespace }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of unknown pods has exceede
d the threshold (0 pods). value={{ $value }} pods, pod={{ $labels.pod }}"
        jp1_pc_resolved_description: "The number of unknown pods has falle
n below the threshold (0 pods). pod={{ $labels.pod }}"
```

- kube_daemonset_failed_number_scheduled#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_daemonset_failed_number_scheduled(Kube state metrics)
     expr: 0 < kube_daemonset_status_desired_number_scheduled - kube_daemo
nset_status_current_number_scheduled
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1205"
        jp1_pc_metricname: "kube_daemonset_status_desired_number_scheduled
, kube_daemonset_status_current_number_scheduled"
        jp1_pc_nodelabel: "{{ $labels.daemonset }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of nodes that failed to exe
cute has exceeded the threshold (0 nodes). value={{ $value }} nodes"
        jp1_pc_resolved_description: "The number of nodes that failed to e
xecute has fallen below the threshold (0 nodes)."
```

- kube_deployment_failed_replicas#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_deployment_failed_replicas(Kube state metrics)
     expr: 0 < kube_deployment_spec_replicas - kube_deployment_status_repl
icas_available
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1206"
        jp1_pc_metricname: "kube_deployment_spec_replicas, kube_deployment
```

```
_status_replicas_available"
        jp1_pc_nodelabel: "{{ $labels.deployment }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of pods that failed to exec
ute on each deployment has exceeded the threshold (0 pods). value={{ $valu
e }} pods"
        jp1_pc_resolved_description: "The number of pods that failed to ex
ecute on each deployment has fallen below the threshold (0 pods)."
```

- kube_replicaset_failed_replicas#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_replicaset_failed_replicas(Kube state metrics)
     expr: 0 < kube_replicaset_spec_replicas - kube_replicaset_status_read
y_replicas
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1207"
        jp1_pc_metricname: "kube_replicaset_spec_replicas, kube_replicaset
_status_ready_replicas"
        jp1_pc_nodelabel: "{{ $labels.replicaset }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of pods that failed to exec
ute on each ReplicaSet has exceeded the threshold (0 pods). value={{ $valu
e }} pods"
        jp1_pc_resolved_description: "The number of pods that failed to ex
ecute on each ReplicaSet has fallen below the threshold (0 pods)."
```

- kube_statefulset_failed_replicas#

```
groups:
 - name: kube_state_metrics
  rules:
   - alert: kube_statefulset_failed_replicas(Kube state metrics)
     expr: 0 < kube_statefulset_replicas - kube_statefulset_status_replica
s_ready
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1208"
        jp1_pc_metricname: "kube_statefulset_replicas, kube_statefulset_st
atus_replicas_ready"
        jp1_pc_nodelabel: "{{ $labels.statefulset }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of pods that failed to exec
ute on each deployment has exceeded the threshold (0 pods). value={{ $valu
e }} pods"
        jp1_pc_resolved_description: "The number of pods that failed to ex
ecute on each deployment has fallen below the threshold (0 pods)."
```

- kube_cron_job_status_failed#

```
groups:
 - name: kube_state_metrics
   rules:
    - alert: kube_cron_job_status_failed(Kube state metrics)
      expr: 0 < kube_job_status_failed * on(job_name, namespace) group_left
(owner_name) kube_job_owner{owner_kind="CronJob", owner_name!="<none>"}
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1209"
        jp1_pc_metricname: "kube_job_status_failed, kube_job_owner"
        jp1_pc_nodelabel: "{{ $labels.owner_name }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The number of pods that failed to exec
ute within a CronJob has exceeded the threshold (0 pods). value={{ $value
}}%"
        jp1_pc_resolved_description: "The number of pods that failed to ex
ecute within a CronJob has fallen below the threshold (0 pods)."
```

- kube_node_status_condition_not_ready#

```
groups:
 - name: kube_state_metrics
   rules:
    - alert: kube_node_status_condition_not_ready(Kube state metrics)
      expr: 1 == sum by (node, instance) (kube_node_status_condition{condit
ion="Ready",status=~"false|unknown"})
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1210"
        jp1_pc_metricname: "kube_node_status_condition"
        jp1_pc_nodelabel: "{{ $labels.node }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The node is in an error state. value={
{ $value }} node"
        jp1_pc_resolved_description: "The node has recovered from its erro
r state."
```

- kube_node_status_condition_memory_pressure#

```
groups:
 - name: kube_state_metrics
   rules:
    - alert: kube_node_status_condition_memory_pressure(Kube state metrics)
      expr: 1 == sum by (node, instance) (kube_node_status_condition{condit
ion="MemoryPressure",status~="true|unknown"}})
       for: 3m
       labels:
         jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
         jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
         jp1_pc_severity: "Error"
         jp1_pc_eventid: "1211"
         jp1_pc_metricname: "kube_node_status_condition"
         jp1_pc_nodelabel: "{{ $labels.node }}"
         jp1_pc_exporter: "JPC Kube state metrics"
         jp1_pc_trendname: "kubernetes"
         job: "jpc_kube_state"
       annotations:
         jp1_pc_firing_description: "The node is in a memory-constrained st
ate. value={{ $value }} node"
         jp1_pc_resolved_description: "The node has recovered from its memo
ry-constrained state."
```

- kube_node_status_condition_disk_pressure#

```
groups:
 - name: kube_state_metrics
   rules:
    - alert: kube_node_status_condition_disk_pressure(Kube state metrics)
      expr: 1 == sum by (node, instance) (kube_node_status_condition{condit
ion="DiskPressure",status=~"true|unknown"})
       for: 3m
       labels:
         jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
         jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
         jp1_pc_severity: "Error"
         jp1_pc_eventid: "1212"
         jp1_pc_metricname: "kube_node_status_condition"
         jp1_pc_nodelabel: "{{ $labels.node }}"
         jp1_pc_exporter: "JPC Kube state metrics"
         jp1_pc_trendname: "kubernetes"
         job: "jpc_kube_state"
       annotations:
         jp1_pc_firing_description: "The node is in a disk-constrained stat
e. value={{ $value }} node"
         jp1_pc_resolved_description: "The node has recovered from its disk
-constrained state."
```

- kube_node_status_condition_pid_pressure#

```
groups:
 - name: kube_state_metrics
   rules:
    - alert: kube_node_status_condition_pid_pressure(Kube state metrics)
      expr: 1 == sum by (node, instance) (kube_node_status_condition{condit
ion="PIDPressure",status=~"true|unknown"})
```

```
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1213"
        jp1_pc_metricname: "kube_node_status_condition"
        jp1_pc_nodelabel: "{{ $labels.node }}"
        jp1_pc_exporter: "JPC Kube state metrics"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kube_state"
      annotations:
        jp1_pc_firing_description: "The node is in a PID assignment-constr
ained state. value={{ $value }} node"
        jp1_pc_resolved_description: "The node has recovered from its PID
assignment-constrained state."
```

- kube_namespace_cpu_percent_used#

```
groups:
 - name: kubelet
  rules:
   - alert: kube_namespace_cpu_percent_used(Kubelet)
     expr: 80 < sum by (namespace, job) (rate(container_cpu_usage_seconds_
total{name!=""}[2m])) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1222"
        jp1_pc_metricname: "container_cpu_usage_seconds_total"
        jp1_pc_nodelabel: "{{ $externalLabels.jp1_pc_prome_clustername }}"
        jp1_pc_exporter: "JPC Kubelet"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kubelet"
        instance: "{{ $externalLabels.jp1_pc_prome_hostname }}"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%, namespace={{ $labels.namespace }}"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%). namespace={{ $labels.namespace }}"
```

- kube_namespace_memory_percent_used#

```
groups:
 - name: kubelet
  rules:
   - alert: kube_namespace_memory_percent_used(Kubelet)
     expr: 80 < sum by (namespace, job) (container_memory_working_set_byte
s and (container_spec_memory_limit_bytes{name!=""} > 0)) / sum by (namespa
ce, job) ((container_spec_memory_limit_bytes{name!=""} > 0) and container_
memory_working_set_bytes) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1223"
        jp1_pc_metricname: "container_memory_working_set_bytes, container_
spec_memory_limit_bytes"
        jp1_pc_nodelabel: "{{ $externalLabels.jp1_pc_prome_clustername }}"
        jp1_pc_exporter: "JPC Kubelet"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kubelet"
        instance: "{{ $externalLabels.jp1_pc_prome_hostname }}"
      annotations:
        jp1_pc_firing_description: "Memory usage has exceeded the threshol
d (80%). value={{ $value }}%, namespace={{ $labels.namespace }}"
        jp1_pc_resolved_description: "Memory usage has fallen below the th
reshold (80%). namespace={{ $labels.namespace }}"
```

- kube_pod_cpu_percent_used_pod#

```
groups:
 - name: kubelet
  rules:
   - alert: kube_pod_cpu_percent_used_pod(Kubelet)
     expr: 80 < sum by (pod, namespace, instance, job) (rate(container_cpu
_usage_seconds_total{name!=""}[2m])) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1220"
        jp1_pc_metricname: "container_cpu_usage_seconds_total"
        jp1_pc_nodelabel: "{{ $labels.pod }}"
        jp1_pc_exporter: "JPC Kubelet"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kubelet"
      annotations:
        jp1_pc_firing_description: "CPU usage has exceeded the threshold (
80%). value={{ $value }}%, pod={{ $labels.pod }}"
        jp1_pc_resolved_description: "CPU usage has fallen below the thres
hold (80%). pod={{ $labels.pod }}"
```

- kube_pod_memory_percent_used#

```
groups:
 - name: kubelet
  rules:
   - alert: kube_pod_cpu_percent_used_pod(Kubelet)
     expr: 80 < sum by (pod, namespace, instance, job) (container_memory_w
orking_set_bytes and (container_spec_memory_limit_bytes{name!=""} > 0)) /
sum by (pod, namespace, instance, job) ((container_spec_memory_limit_bytes
{name!=""} > 0) and container_memory_working_set_bytes) * 100
      for: 3m
      labels:
        jp1_pc_product_name: "/HITACHI/JP1/JPCCS2"
        jp1_pc_component: "/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO"
        jp1_pc_severity: "Error"
        jp1_pc_eventid: "1221"
        jp1_pc_metricname: "container_memory_working_set_bytes, container_
spec_memory_limit_bytes"
        jp1_pc_nodelabel: "{{ $labels.pod }}"
        jp1_pc_exporter: "JPC Kubelet"
        jp1_pc_trendname: "kubernetes"
        job: "jpc_kubelet"
      annotations:
        jp1_pc_firing_description: "Memory usage has exceeded the threshol
d (80%). value={{ $value }}%, pod={{ $labels.pod }}"
        jp1_pc_resolved_description: "Memory usage has fallen below the th
reshold (80%). pod={{ $labels.pod }}"
```

#

When defining multiple alerts with the same integrated agent host, avoid specifying duplicate groups:, or specifying a name that specifies the same group name in duplicate. In "alert", specify the value of the alert definition while following the naming rule given below. If you do not follow the rule, the JP1 event will not be created.

alert: metric-definition-name(exporter-name)any-value

Node exporter discovery configuration file (jpc_file_sd_config_node.yml)

Format

Write in YAML format.

```
- targets:
  - Monitored hostname:Port number of the Node exporter
  labels:
    jp1_pc_exporter: JPC Node Exporter
    jp1_pc_category: platform
    jp1_pc_trendname: node_exporter
    jp1_pc_multiple_node: "{__name__=~'node_systemd_unit_.*'}"#
```

#

Parameters for service monitoring that are set in the model file by JP1/IM - Agent 13-01 or later installer.

If you are upgrading from JP1/IM - Agent 13-00 to 13-01 or later and want to use the service monitoring feature, add the jp1_pc_multiple_node parameters manually. For details, see *2.19.2(3)(f) Configuring service monitor settings (for Linux) (Optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

File

`jpc_file_sd_config_node.yml`

`jpc_file_sd_config_node.yml.model` (model file)

Storage directory

■Integrated agent host

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This is a file that configures the Node exporter that Prometheus server scrapes.

Character code

UTF-8 (without BOM)

Line feed code

LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *Monitored hostname*:*Port number of the Node exporter*

  Specify "*Monitored hostname*:*Port number of the Node exporter*" as characters other than 1 to 2,595 control characters.

  The monitored host name is required and specified. The specified monitored host name is set in the monitoring agent installation script. You can also specify the FQDN format.

  If you have changed the port number of the Node exporter from the initial value, change the value of the *Port number of the Node exporter*.

Process exporter discovery configuration file (jpc_file_sd_config_process.yml)

Syntax

Written in YAML format.

```
- targets:
  - installation-host-name:Process-exporter-port-number
  labels:
    jp1_pc_exporter: JPC Process exporter
    jp1_pc_category: platform
    jp1_pc_trendname: process_exporter
    jp1_pc_multiple_node: "{__name__=~'namedprocess_namegroup_.*'}"
    jp1_pc_agent_create_flag: false
```

File

`jpc_file_sd_config_process.yml`

`jpc_file_sd_config_process.yml.model` (Model file)

Storage directory

When using a physical host

`/opt/jp1ima/conf/`

When using a logical host

shared-directory`/jp1ima/conf/`

Description

This file configures the Process Exporter to be scraped by the Prometheus server.

Character encoding

UTF-8 (without BOM)

Linefeed code

LF

Timing in which definitions are reflected

The Process Exporter becomes a target for scraping when executing or restarting the Prometheus server reload API. Following this, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

`-` *installation-host-name*`:`*Process-exporter-port-number*

The *installation-host-name* is set based on the installation script for the integrated agent. This can also be specified in FQDN format.

If the Process exporter port number has changed from its default value, change the *Process-exporter-port-number* value after the colon (`:`).

Specify the *installation-host-name*`:`*Process-exporter-port-number* using 1 to 2,574 characters, excluding control characters.

Windows exporter discovery configuration file (jpc_file_sd_config_windows.yml)

Format

Write in YAML format.

```
- targets:
  - Monitored hostname:Port number of the Windows exporter
  labels:
    jp1_pc_exporter: JPC Windows Exporter
    jp1_pc_category: platform
    jp1_pc_trendname: windows_exporter
    jp1_pc_multiple_node: "{__name__=~'windows_process_.*|windows_service_.*
'}"#
```

#

Parameters that JP1/IM - Agent 13-01 or later installer sets in the model file for process monitoring and service monitoring.

If you are upgrading from JP1/IM - Agent 13-00 to 13-01 or later and want to use the service monitoring feature, add the jp1_pc_multiple_node parameters manually. For details, see *1.21.2(3)(f) Configuring service monitoring settings (for Windows) (Optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

File

`jpc_file_sd_config_windows.yml`

`jpc_file_sd_config_windows.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`/jp1ima/conf/`

Description

This is a file that configures the Windows exporter that Prometheus server scrapes.

Character code

UTF-8 (without BOM)

Line feed code

CR+LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *Monitored hostname*:*Port number of the Windows exporter*

  Specify "*Monitored hostname*:*Port number of the Windows exporter*" as characters other than 1 to 2,595 control characters.

  The monitored host name is required and specified. The specified monitored host name is set in the monitoring agent installation script. You can also specify the FQDN format.

  If you have changed the port number of the Windows exporter from the initial value, change the value of the *Port number of the Windows exporter*.

Node exporter for AIX discovery configuration file (jpc_file_sd_config_node_aix.yml)

Format

Write in YAML format.

```
- targets:
  - Monitored hostname: Port number of the Node exporter for AIX
  ...
  labels:
    jp1_pc_exporter: JPC Node exporter for AIX
    jp1_pc_category: platform
    jp1_pc_trendname: node_exporter_aix
```

File

`jpc_file_sd_config_node_aix.yml`

`jpc_file_sd_config_node_aix.yml.model (model file)`

Storage directory

- Integrated agent host

  In Windows:

  - For a physical host

    Agent-path`\conf\`

  - For a logical host

    shared-folder`\jp1ima\conf\`

  In Linux:

  - For a physical host

    `/opt/jp1ima/conf/`

  - For a logical host

    shared-directory`/jp1ima/conf/`

Description

This is a file that configures the Node Exporter for AIX that the Prometheus server scrapes.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected

Information that is specified

Monitored host name

Specifies the host name of the monitored host (AIX) in characters other than 1 to 255 control characters. You can also specify FQDN format. "localhost" cannot be specified.

Node exporter for AIX port number

Specifies the port number of Node exporter for AIX to scrape to.

Example definition

```
- targets:
  - hostA:20730
  - hostB:20730
  labels:
    jp1_pc_exporter: JPC Node exporter for AIX
    jp1_pc_category: platform
    jp1_pc_trendname: node_exporter_aix
```

Blackbox exporter (HTTP/HTTPS monitoring) discovery configuration file (jpc_file_sd_config_blackbox_http.yml)

Format

Write in YAML format.

```
- targets:
  - Monitored hostname:IM Management Node Label Name:URL
  ...
  labels:
    jp1_pc_exporter: JPC Blackbox Exporter
    jp1_pc_category: serviceResponse
    jp1_pc_trendname: blackbox_exporter
    jp1_pc_remote_monitor_instance: install-host-name: Synthetic metric coll
ector(Blackbox exporter)
```

File

`jpc_file_sd_config_blackbox_http.yml`

`jpc_file_sd_config_blackbox_http.yml.model` (model file)

`file_sd_config_blackbox_`*module-name-start-with-http*`.yml` (user-created)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

A file that configures the Blackbox exporter that Prometheus server scrapes with HTTP/HTTPS monitoring.

If you have newly defined a module in Process exporter configuration file (jpc_blackbox_exporter.yml) HTTP/HTTPS monitoring, create a discovery configuration file with the following name and copy the model file for this discovery configuration file, depending on the target:

`file_sd_config_blackbox_`*module-name*`.yml`

For details on Blackbox exporter monitoring setup, see *1.21.2(6) Setup of Blackbox exporter* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *Monitored hostname***:***IM Management Node Label Name***:***URL*

  Monitored hostname, *IM Management Node Label Name*, and *URL* are separated by a ":" (colon).

  The *Monitored hostname* is a character other than 1 to 255 control characters, and specifies the host name of the web server to be monitored. You can also specify the FQDN format. "localhost" cannot be specified.

  The *IM Management Node Label Name* is a character that does not include 1 to 255 characters ":" (colon) and control characters, and specifies the string to be displayed in the IM Manager label name in the Integrated Operations Viewer. Make sure that the string when encoding the URL cannot exceed 234 bytes (the upper limit is 26 characters when all multibyte characters are used).

  A *URL* is a character other than 1 to 2083 control characters that specifies URL to monitor. You can specify IP address instead of Host name in URL, but if you specify IP address, you cannot Enable validation of the monitored certificate (you cannot false in the insecure_skip_verify of Process exporter configuration file (jpc_blackbox_exporter.yml) tls_config). In addition, the following metric cannot be monitored because "true" is Setup to the insecure_skip_verify of the tls_config of Process exporter configuration file (jpc_blackbox_exporter).

  - probe_ssl_last_chain_expiry_timestamp_seconds

Example definition

```
- targets:
  - hostB: Metric forwarder(Prometheus server) healthy:http://hostB:20713/-/healthy
  - hostB: Alert forwarder(Alertmanager) healthy:http://hostB:20714/-/healthy
  labels:
    jp1_pc_exporter: JPC Blackbox Exporter
    jp1_pc_category: serviceResponse
    jp1_pc_trendname: blackbox_exporter
    jp1_pc_remote_monitor_instance: hostA: Synthetic metric collector(Blackbox exporter)
```

Blackbox exporter (ICMP monitoring) discovery configuration file (jpc_file_sd_config_blackbox_icmp.yml)

Format

Write in YAML format.

```
- targets:
  - Host name or IP address of the monitored host
  ...
  labels:
    jp1_pc_exporter: JPC Blackbox Exporter
    jp1_pc_category: platform
    jp1_pc_trendname: blackbox_exporter
    jp1_pc_remote_monitor_instance: install-host-name: Synthetic metric coll
ector(Blackbox exporter)
```

File

`jpc_file_sd_config_blackbox_icmp.yml`

`jpc_file_sd_config_blackbox_icmp.yml.model` (model file)

`file_sd_config_blackbox_`*module-name-start-with-icmp*`.yml` (user-created)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This file configures the Blackbox exporter that Prometheus server scrapes with ICMP monitoring.

If you have newly defined a module in Process exporter configuration file (jpc_blackbox_exporter.yml) ICMP monitoring, create a discovery configuration file with the following name and Copy the model File for this discovery configuration file, depending on the target:

`file_sd_config_blackbox_`*module-name*`.yml`

For details on Blackbox exporter monitoring setup, see *1.21.2(6) Setup of Blackbox exporter* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *Host name or IP address of the monitored host*

  Specifies the host name or IP address of the monitored host in characters other than 1 to 2,595 control characters. You can also specify the FQDN format. "localhost" cannot be specified.

  When displayed in the Integrated Operations Viewer, the string specified for the host name or internet address of the monitored host is displayed as the label of the IM management node of the agent host SID. If you want to specify an IP address for the host to be monitored and display the host name in the label of the IM management node, set the host name definition file (imdd_host_name.conf) of JP1/IM - Manager and map the IP address to the host name. For details about the host name definition file, see *Host name definition file (imdd_host_name.conf)*.

Example definition

```
- targets:
  - hostB
  - hostC
  labels:
    jp1_pc_exporter: JPC Blackbox Exporter
    jp1_pc_category: platform
    jp1_pc_trendname: blackbox_exporter
    jp1_pc_remote_monitor_instance: hostA: Synthetic metric collector(Blackb
ox exporter)
```

Yet another cloudwatch exporter discovery configuration file (jpc_file_sd_config_cloudwatch.yml)

Format

Write in YAML format.

```
- targets:
  - Monitoring agent host name:Yet another cloudwatch exporter port number
  labels:
    jp1_pc_exporter: JPC YA Cloudwatch Exporter
    jp1_pc_trendname: ya_cloudwatch_exporter
    jp1_pc_remote_monitor_instance: Monitoring agent host name: AWS metric c
ollector(Yet another cloudwatch exporter)
```

File

`jpc_file_sd_config_cloudwatch.yml`

`jpc_file_sd_config_cloudwatch.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This is a file that configures the Yet another cloudwatch exporter that the Prometheus server scrapes.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *Monitoring agent host name*:*Yet another cloudwatch exporter port number*

  Set the *Monitoring agent host name* to the host name where the monitoring module was installed when the monitoring agent was installed. You can also specify the FQDN format.

  If you have changed the port number of Yet another cloudwatch exporter from the initial value, change the value of the *Yet another cloudwatch exporter port number*.

Promitor discovery configuration file (jpc_file_sd_config_promitor.yml)

Syntax

Written in YAML format.

```
- targets:
  - installation-host-name:Promitor-Scraper-port-number
  labels:
    jp1_pc_exporter: JPC Promitor
    jp1_pc_trendname: promitor
    jp1_pc_remote_monitor_instance: installation-host-name:Azure metric coll
ector (Promitor)
jp1_pc_rm_agent_create_flag: false
```

File

jpc_file_sd_config_promitor.yml

jpc_file_sd_config_promitor.yml.model (Model file)

Storage directory

For Windows

When using a physical host

Agent-path\conf\

When using a logical host

shared-folder\jp1ima\conf\

For Linux

When using a physical host

/opt/jp1ima/conf/

When using a logical host

shared-directory/jp1ima/conf/

Description

This file configures the Promitor to be scraped by the Prometheus server.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

The Promitor becomes a target for scraping when executing or restarting the Prometheus server reload API. Following this, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

- *installation-host-name*:*Promitor-Scraper-port-number*

  The *installation-host-name* is set based on the installation script for the integrated agent. This can also be specified in FQDN format.

  If the Promitor Scraper port number has changed from its default value, change the *Promitor-Scraper-port-number* value after the colon (`:`).

OracleDB exporter discovery configuration file (jpc_file_sd_config_oracledb.yml)

Format

Write in YAML format.

```
- targets:
  - Oracle Database hostname:Monitored name:OracleDB exporter port number
  ...
  labels:
    jp1_pc_exporter: JPC OracleDB exporter
    jp1_pc_category: database
    jp1_pc_trendname: oracledb_exporter
    jp1_pc_remote_monitor_instance: install-host-name:OracleDB metric collec
tor(OracleDB exporter)
```

File

`jpc_file_sd_config_oracledb.yml`

`jpc_file_sd_config_oracledb.yml.model` (model file)

Storage directory

- Integrated agent host

  In Windows:

  - For a physical host

    Agent-path`\conf\`

  - For a logical host

    shared-folder`\jp1ima\conf\`

  In Linux:

  - For a physical host

    `/opt/jp1ima/conf/`

  - For a logical host

    shared-directory`/jp1ima/conf/`

Description

This is a file that configures the OracleDB exporter that Prometheus server scrapes.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

Oracle Database hostname

Specify the hostname of Oracl**e Database**, between 1 and 253 characters. You can also specify FQDN format. "localhost" cannot be specified.

Monitored name

Specifies an optional name to distinguish between monitored objects. Specifies a character string that is not a colon (:) or control character and that appears in IM management node labelname for integrated operation viewer. When URL is encoded, the character string must be between 1 and 234 bytes (the upper limit for all multibyte characters is 26 characters).

OracleDB exporter port-number

Specifies the port number of OracleDB exporter to scrape to.

Hostname to install to

Specifies the host name of the host on which OracleDB exporter is running.

Definition example

```
- targets:
  - ORAHOST1:Accounting department DB:30001
  - ORAHOST1:Human resources DB:30002
  labels:
    jp1_pc_exporter: OracleDB Exporter
    jp1_pc_category: database
    jp1_pc_trendname: oracledb_exporter
    jp1_pc_remote_monitor_instance: hostA: OracleDB metric collector(OracleD
B exporter)
```

Script exporter discovery configuration file (jpc_file_sd_config_script.yml)

Syntax

Written in YAML format.

```
- targets:
  - installation-host-name:Script-exporter-port-number
  labels:
    jpc_pc_exporter: JPC Script exporter
    jpc_pc_trendname: script_exporter
    jp1_pc_multiple_node: "{job='jpc_script.*',jp1_pc_multiple_node=''}"
    jp1_pc_agent_create_flag: false
```

File

`jpc_file_sd_config_script.yml`

`jpc_file_sd_config_script.yml.model` (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\`

When using a logical host

shared-folder`\jp1ima\conf\`

For Linux

When using a physical host

`/opt/jp1ima/conf/`

When using a logical host

shared-directory`/jp1ima/conf/`

Description

This file configures the Script exporter to be scraped by the Prometheus server.

When Script exporter discovery is specified using the file-based *file_sd_config* method, specify this file to file_sd_configs in scrape_configs in the Prometheus configuration file (jpc_prometheus_server.yml).

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

The Script exporter becomes a target for scraping when executing or restarting the Prometheus server reload API. Following this, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

- *installation-host-name*:*Script-exporter-port-number*

  The *installation-host-name* is set based on the installation script for the integrated agent. This can also be specified in FQDN format.

  If the Script exporter port number has changed from its default value, change the *Script-exporter-port-number* value after the colon (:).

User-specific discovery configuration file (user_file_sd_config_any-name.yml)

Format

Write in YAML format.

```
- targets:
  - monitored host name[:Any string]
  ...
  labels:
[    jp1_pc_exporter: Any exporter name that does not start with "JPC"]
[    jp1_pc_category: IM Management Node Category ID]
[    jp1_pc_trendname: Prometheus Trend Name]
[    jp1_pc_remote_monitor_instance: Installation Hostname:The string to dis
play in the label of the IM Management node]
[    jp1_pc_rm_agent_create_flag: Remote-agent-SID-creation-flag]
[    jp1_pc_agent_create_flag: agent-SID-creation-flag]
[    jp1_pc_multiple_node: condition-for-get-label-set-for-multiple-IM-manag
ement-node-creation]
```

File

`user_file_sd_config_`*any-name*`.yml`

Storage directory

It can be stored in any directory. However, when storing under the directory where the monitoring agent is installed, store it in the following directory.

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This is a file that sets what Prometheus server scrapes. User-created exporters can also be subject to scraping.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the Prometheus server reload API is executed or restarted, the Prometheus server is subject to scraping. Then, when the jddcreatetree and jddupdatetree commands are executed, the contents of the tree display in the integrated operations viewer are reflected.

Information that is specified

- *monitored host name*[:*Any string*]

  Specify "*monitored host name*[:*Any string*]" as characters other than 1 to 2,574 control characters.

  The *monitored host name* is a character other than 1 to 255 control characters and is specified as required. You can also specify the FQDN format. "localhost" cannot be specified.

  Specify any string if other specifications are required in the Exporter specification.

  In Prometheus configuration file (jpc_prometheus_server.yml) scrape definition, relabel_configs is Setup and the required string is passed as an argument at scrape time.

  If you have more than 2,574 characters, in Prometheus configuration file (jpc_prometheus_server.yml) relabel_configs, replace instance labeled Value with a non-control character from 1 to 2574. Note that instance label Value must be specified in the format of "Monitored Host name: Arbitrary character string" and must not overlap with Value of other instance labels in the same monitoring agent host.

  For setup of the relabel_configs, see the section describing *Information that is specified* in *Prometheus configuration file (jpc_prometheus_server.yml)*.

`jp1_pc_exporter:` *Any exporter name that does not start with "JPC"*

For *Any exporter name that does not start with "JPC"*, specify the character string to be displayed in the properties of the jp1_pc_exporter in the property display with characters other than 1 to 255 control characters. If omitted, "Unknown Exporter" is displayed.

`jp1_pc_category:` *category-ID-for-IM-management-node*

For the *category-ID-for-IM-management-node*, specify the IM Management node category identifier of the agent SID in characters other than 1 to 255 control characters.

If the specification is omitted, "otherApplications" is assumed to be specified.

`jp1_pc_trendname:` *Prometheus-trend-name*

For *Prometheus-trend-name*, specify the Prometheus trend name of the metric definition file to be displayed on the IM management node of the agent SID in characters other than 1 to 255 control characters.

If the specification is omitted, job labeled Value is turned Setup.

`jp1_pc_remote_monitor_instance:` *install-host-name-string-to-be-labeled-with-IM-management-node*

Specify only for exporters that you want to monitor remotely. A remotely monitored exporter is an exporter that monitors a host other than the one on which the exporter is set up.

For the installation host name, specify the host name on which the exporter was installed, in characters other than 1 to 255 control characters.

The string to be displayed on the label of IM management node is the string to be displayed on the label of IM management node in Remote Monitoring service SID with a control character and a character other than a colon. Because a colon is a delimiter, if specified, the string after the last specified colon is subject to the string labeled IM management node. When URL is encoded, the character string must be 234 bytes or less (the upper limit for multibyte characters is 26).

Specify a colon delimiter between the install Host name and the string labeled in IM management node. If not specified, it performs considering Installed Host name and the text labeled in IM management node identical.

If you omit this option, the utility does not create an Remote Monitoring serviced SID.

`jp1_pc_rm_agent_create_flag: Remote agent SIDs Creation Flag`

Specify this option only for Exporter monitored by remote. Specify true or false. It is not case sensitive. If no jp1_pc_remote_monitor_instance is specified, this Setup is ignored.

- true

  Create a IM management node for "Remote agent SID" in units of "agent host SID" and "Monitored Host name: Any String".

- false

  Do not create IM management node for "Remote agent SID" in units of "agent host SID" and "Monitored Host name: Any String".

If a character other than true or false is specified, or the specified character is omitted, the utility assumes that true is specified.

`jp1_pc_agent_create_flag: creation flag of agent SID`

Specify this option only for Exporter is monitoring the host where Exporter is installed. Specify true or false. It is not case sensitive. If the jp1_pc_remote_monitor_instance is specified, this Setup is ignored.

- true

  Create a IM management node for "agent SID" in units of "Monitored Host name: Any String".

- false

  Do not create a IM management node for agent SID in units of "Monitored Host name: Any String".

If a character other than true or false is specified, or the specified character is omitted, the utility assumes that true is specified.

`jp1_pc_multiple_node:` Condition for Get Label Set for Multiple IM management node Creation

Specifies that more than one IM management node (agent SIDs or Remote agent SIDs) is to be created for the "Monitored Host name: Any String." Specifies the conditions to obtain the labels required to create IM management node from Trend data Management Database.

You can specify only one condition. For details about Value that can be specified, see the description of match parameter in *4.5.18 jp1TrendDataService.getLabelList*.

If this option is omitted, the utility does not create more than one IM management node (agent SIDs or Remote agent SIDs) for the "Monitored Host name: Any String".

Example definition

```
- targets:
  - hostA:9256
  labels:
    jp1_pc_exporter: Process Exporter
    jp1_pc_category: platform
    jp1_pc_trendname: process
```

Service definition file (jpc_program-name_service.xml)

Format

```
<service>
  <id>service-ID</id>
  <name>display-name-of-the-service</name>
  <description>description</description>
  <workingdirectory>working-directory</workingdirectory>
  <env name="environment-variable-name" value="value"></env>
  <executable>"program-path"</executable>
  <arguments>arguments-of-the-program</arguments>
  <startmode>type-of-startup</startmode>
  <logpath>log-output-directory</logpath>
  <log mode="roll-by-size">
    <sizeThreshold>log-file-size</sizeThreshold>
    <keepFiles>Number of log faces</keepFiles>
  </log>
  <stoptimeout>Termination timeout period</stoptimeout>
</service>
```

File

- For a physical host
  `jpc_`*program-name*`_service.xml`
  `jpc_`*program-name*`_service.xml.model` (model file)
- For a logical host
  `jpc_`*program-name*`_service_`*logical-host-name*`.xml`

Storage directory

■Integrated agent host

- For a physical host (Model File storage destination)
  Agent-path`\conf\`
- For Physical host and Logical host (storage destination of definition file)
  Agent-path`\bin\`

Description

This is the definition file of the Windows serviced program.

Character code

UTF-8 (without BOM)

Line feed code

CR+LF

When the definitions are applied

If you change <startmode> in the definition file, it will take effect by reinstalling the service. For each JP1/IM agent control base or add-on program service, reinstall the service using the commands listed in the following tables.

Add-on program or JP1/IM agent control base	Service name	Command
Prometheus server	jpc_prometheus_server_service.exe	jpc_prometheus_server_service.exe
Alertmanager	jpc_alertmanager_service.exe	jpc_alertmanager_service.exe
Windows exporter	jpc_windows_exporter_service.exe	jpc_windows_exporter_service.exe
Blackbox exporter	jpc_blackbox_exporter_service.exe	jpc_blackbox_exporter_service.exe
Yet another cloudwatch exporter	jpc_ya_cloudwatch_exporter_service.exe	jpc_ya_cloudwatch_exporter_service.exe
Promitor	jpc_promitor_scraper_service.exe	jpc_promitor_scraper_service.exe
	jpc_promitor_resource_discovery_service.exe	jpc_promitor_resource_discovery_service.exe
Script exporter	jpc_script_exporter_service.exe	jpc_script_exporter_service.exe
Fluentd	jpc_fluentd_service.exe	jpc_fluentd_service.exe
imagent	jpc_imagent_service.exe	jpc_imagent_service.exe
imagentproxy	jpc_imagentproxy_service.exe	jpc_imagentproxy_service.exe
imagentaction	jpc_imagentaction_service.exe	jpc_imagentaction_service.exe

If you change the <arguments> or <stoptimeout> of File, it is reflected by Restart of theservice.

Information that is specified

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
<service>	Configure the service settings.	--	--	--
<id>	Specify the ID of the service (the ID that Windows uses internally to identify the service) (required). This identifier must be unique among all services installed on the system and must consist entirely of alphanumeric characters.	N	--	• For Prometheus server jpc_prometheus • For Alertmanager jpc_alertmanager • For Windows exporter jpc_windows_exporter • For Blackbox exporter jpc_blackbox_exporter • For JP1/IM agent control base (imagent) jpc_imagent • For JP1/IM agent control base (imagentproxy) jpc_imagentproxy • For JP1/IM agent control base (imagentaction) jpc_imagentaction • For Fluentd jpc_fluentd

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
					• For Yet another cloudwatch exporter: jpc_ya_cloudwatch_exporter • For Promitor Scraper: jpc_promitor_scraper • For Promitor Resource Discovery: jpc_promitor_resource_discovery • For Script exporter: jpc_script_exporter • For OracleDB exporter oracledb_exporter_instance name
	<name>	Specify a display name for the service (the short display name of the service) (optional). It can contain spaces and other characters. Do not specify a long string, such as <id>. It must also be unique among all services in a particular system.	N	--	• For Prometheus server JP1/IM3-Agent Metric forwarder • For Alertmanager JP1/IM3-Agent Alert forwarder • For Windows exporter JP1/IM3-Agent Windows metric collector • For Blackbox exporter JP1/IM3-Agent Synthetic metric collector • For JP1/IM agent management base (imbase) ■For normal hosts JP1/IM-Agent Base Server ■For cluster environments JP1/IM-Agent Base Server_ Name. Logical host • For JP1/IM agent management base (imbaseproxy) ■For normal hosts JP1/IM-Agent Base Proxy Server ■For cluster environments JP1/IM-Agent Base Proxy Server_ Name. Logical host • For JP1/IM agent control base (imagent) JP1/IM3-Agent

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
					• For JP1/IM agent control base (imagentproxy) JP1/IM3-Agent proxy • For JP1/IM agent control base (imagentaction) JP1/IM3-Agent action • For Fluentd JP1/IM3-Agent Log trapper • For Yet another cloudwatch exporter: JPC YA Cloudwatch exporter • For Promitor Scraper: JPC Promitor Scraper • For Promitor Resource Discovery: JPC Promitor Resource Discovery • For Script exporter: JPC Script exporter • For OracleDB exporter OracleDB metric collector instance name
	<description>	Specify a description (long description) (optional). This description is displayed in the Windows Service Control Manager when the service is selected.	N	--	• For Prometheus server Prometheus server • For Alertmanager Alertmanager • For Windows exporter windows_exporter • For Blackbox exporter blackbox_exporter • For JP1/IM agent management base (imbase) JP1 IMA Base Service • For JP1/IM agent management base (imbaseproxy) JP1 IMA Base Proxy Service • For JP1/IM agent control base (imagent) JPC IM-Agent Service • For JP1/IM agent control base (imagentproxy) JPC IM-Agent Proxy Service • For JP1/IM agent control base (imagentaction) JPC IM-Agent Action Service • For Fluentd Fluentd

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
					- For Yet another cloudwatch exporter: jpc_ya_cloudwatch_exporter - For Promitor Scraper: jpc_promitor_scraper - For Promitor Resource Discovery: jpc_promitor_resource_discovery - For Script exporter: jpc_script_exporter - For OracleDB exporter OracleDB exporter
	<workingdirectory>	Specify the working directory (the current directory of the service).	N	--	- For Prometheus server,Alertmanager,Windows exporter, and Blackbox exporter Automatically Setup during set-up. - For JP1/IM agent management base (imbase and imbaseproxy) *Manager-path*`\bin\imdd\imagent` - For JP1/IM agent control base (imagent,imagentproxy, and imagentaction) and Fluentd *Agent-path*`\bin`
	<env name="*environment-variable-name*" value="*value*">	Specifies the *environment-variable-name* and its *value*. This is specified for Promitor Scraper, Promitor Resource Discovery, and OracleDB exporter.	- For Promitor Scraper and Promitor Resource Discovery N - For OracleDB exporter Y	--	- For Promitor Scraper: name="PROMITOR_CONFIG_FOLDER" value="*installation-directory*/jp1ima/conf/promitor/scraper" - For Promitor Resource Discovery: name="PROMITOR_CONFIG_FOLDER" value="*installation-directory*/jp1ima/conf/promitor/resource-discovery" - For OracleDB exporter See the *Preparing to add a monitoring target* in *1.23.1(4)(a) Adding a monitoring target (Required)* in the *JP1/Integrated Management*

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
					3 - Manager Configuration Guide.

	<executable>	Specify the path of the program (the path of the executable file to be launched) (required).
		You can specify an absolute path or specify the executable file name to search from PATH.
		Note, however, that services often run under different user accounts, so they may have a different PATH than the shell.
		Note that specifying an empty string does not result in an error.
			N	--	• For Prometheus server
					prometheus.exe
					• For Alertmanager
					alertmanager.exe
					• For Windows exporter
					windows_exporter.exe
					• For Blackbox exporter
					blackbox_exporter.exe
					• For JP1/IM agent management base (imbase)
					imbase
					• For JP1/IM agent management base (imbaseproxy)
					imbaseproxy
					• For JP1/IM agent control base (imagent)
					imagent
					• For JP1/IM agent control base (imagentproxy)
					imagentproxy
					• For JP1/IM agent control base (imagentaction)
					Imagentaction
					• For Fluentd
					Agent-path`\lib\ruby\ruby.exe`
					• For Yet another cloudwatch exporter:
					`ya_cloudwatch_exporter.exe`
					• For Promitor Scraper:
					`promitor_scraper.exe`
					• For Promitor Resource Discovery:
					`promitor_resource_discovery.exe`
					• For Script exporter:
					`script_exporter.exe`
					• For OracleDB exporter:
					destination-folder`\oracledb_exporter_windows\jp1ima\bin\oracledb_exporter.exe`

	<arguments>	Specify the program arguments (the arguments to be passed to the executable file to be launched).	Y	Change the settings when you want to change the arguments.	• For Prometheus server

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
		If you want to change the value, restart the service after changing the value.			For prometheus.exe parameters, see prometheus Command Options. `--Config.file = "`*`Agent-path`*`/conf/jpc_prometheus_server.yml"` - For Alertmanager About arguments of alertmanager.exe, see *alertmanager command options*. - For Windows exporter About arguments of windows_exporter.exe, see *windows_exporter command options*. - For Blackbox exporter About arguments of blackbox_exporter.exe, see *blackbox_exporter command options*. - For JP1/IM agent management base (imbase and imbaseproxy) and JP1/IM agent control base (imagent, imagentproxy, and imagentaction) ■For normal hosts None ■For cluster environments -hostname *logical host name* - For Fluentd For details about the parameters of fluentd command, see *fluentd command options* - For Yet another cloudwatch exporter: For details on the ya_cloudwatch_exporter.exe arguments, see *ya_cloudwatch_exporter command options*. - For Promitor Scraper: For details on the promitor_scraper.exe arguments, see *promitor_scraper command options*. - For Promitor Resource Discovery:

Item			Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
						For details on the promitor_resource_discovery.exe arguments, see *promitor_resource_discovery command options*. • For Script exporter: For details on the script_exporter.exe arguments, see *script_exporter command options*. • For OracleDB exporter For information about oracledb_exporter.exe arguments, see *oracledb_exporter command options*.
	<startmode>		Specify the startup type (Windows service start mode) (optional). Specify one of the following values: • Automatic • Manual If you want to change the value, uninstall the service once, change the value, and then reinstall the service.	Y	• For Prometheus server,Alertmanager, Windows exporter,Blackbox exporter, JP1/IM agent control base (imagent, and imagentproxy), Fluentd, and OracleDB exporter For clustered operation, specify Manual.	• For Prometheus server,Alertmanager,Windows exporter, Blackbox exporter, Yet another cloudwatch exporter, Promitor Scraper, Promitor Resource Discovery, Script exporter, JP1/IM agent control base (imagent, and imagentproxy) and Fluentd Automatic • For JP1/IM agent management base (imbase and imbaseproxy) Manual
	<logpath>		Specify the log output destination directory (the directory where the log file will be created). If specified, the directory where the configuration file exists is the default. If you want to change the value, restart the service after changing the value.	Y	--	Set up automatically during setup.
	<log mode="roll-by-size">		The log output mode is roll-by-size mode. It operates in the same way as append mode, but if the value set for log file size is exceeded, it will be rolled to myapp.1.out.log, myapp.2.out.log, etc.	N	--	--
		<sizeThreshold>	Specify it in KB when changing the log file size (rotation threshold).	N	Change Setup when you are prompted to change Value from the support desk.	10240

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	If you want to change the value, restart the service after changing the value.			
<keepFiles>	Specify this when changing the number of log planes (the number of role files to keep). A log with the specified number of sides + 1 side is created. If you want to change the value, restart the service after changing the value. Value that can be Setup is 7 to 511.	Y	Change Setup when you are prompted to change Value from the support desk.	7 (99 for Fluentd only)
<stoptimeout>	Specifies the wait time to stop the service (the maximum amount of time to wait after issuing a stop request to the program before the service is stopped). If you want to change the value, restart the service after changing the value.	Y	Change the settings when you want to change the waiting time for an outage.	• For Prometheus server 110sec • For Alertmanager,Windows exporter,Blackbox exporter, Yet another cloudwatch exporter, Promitor Scraper, Promitor Resource Discovery, Script exporter, and Fluentd 60sec • For JP1/IM agent management base (imbase), and JP1/IM agent control base (imagent) 90sec • For JP1/IM agent management base (imbaseproxy), and JP1/IM agent control base (imagentproxy) 140sec • For OracleDB exporter 60sec

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- prometheus command options

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--config.file="jpc_prometheus_server.yml"	Specifies the path to the Prometheus configuration file.	Y	--	--config.file="*Agent-path*/jp1ima/conf/jpc_prometheus_server.yml"
--web.listen-address="0.0.0.0:9090"	Specify the listening port. If you want to limit the listening IP address, also include the host name or internet address. If you	Y	Specify this when you want to change the port	--web.listen-address="0.0.0.0:20713"

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	specify a host name, you can specify up to 255 bytes. <Configuration example> To accept requests for all IP addresses, set the following: --web.listen-address="0.0.0.0:20713" If you want to limit the IP addresses that are accepted, you can specify a host name or an internet address as follows: --web.listen-address="*host-name-or-IP-address*:20713"		or limit the listening IP address.	
--web.read-timeout=5m	Specifies the maximum amount of time before reading requests times out and idle connections are closed.	N	--	--web.read-timeout=5m
--web.max-connections=512	Specifies the maximum number of concurrent connections.	N	--	--web.max-connections=10
--web.enable-lifecycle	Specifies to enable shutdown and reload by HTTP request.	N	--	--web.enable-lifecycle
--storage.tsdb.path="data/"	Specify the path where you want to save the performance data.	N	--	--storage.tsdb.path="data/prometheus_server/"
--storage.tsdb.min-block-duration=2h	Specifies the minimum duration of the block.	N	--	--storage.tsdb.min-block-duration=1h
--storage.tsdb.max-block-chunk-segment-size=512MB	Specifies the maximum size of a single chunk segment in a block.	N	--	--storage.tsdb.max-block-chunk-segment-size=32MB
--storage.tsdb.retention.time=STORAGE.TSDB.RETENTION.TIME	Specify the retention period of performance data in hours in the range of 1 to 48h. <Configuration example> --storage.tsdb.retention.time=24h	Y	If a range vector selector is used for the alert rule condition, specify a value greater than that range.	--storage.tsdb.retention.time=1h
--storage.remote.flush-deadline=<duration>	Specify the maximum waiting time when stopping when remote lights and alerts cannot be sent.	N	--	--storage.remote.flush-deadline=5s
--rules.alert.for-outage-tolerance=1h	Specifies the maximum Prometheus server outage period for which the alert "pending" state can be restored.	N	--	--rules.alert.for-outage-tolerance=1h
--rules.alert.for-grace-period=10m	Specifies the minimum duration of the "for" state when restored from an alert. Valid only for alerts that have a longer "for" time than this option.	N	--	--rules.alert.for-grace-period=10m
--log.level=info	Only messages above the specified level are logged. You can specify one of the following levels: debug, info, warn, or error.	N	Change Setup when you are prompted to change Value from the support desk. Normally, no change is required.	--log.level=debug

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- alertmanager command options

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--config.file="jpc_alertmanager.yml"	Specifies the path to the Alertmanager configuration file.	Y	--	--config.file="*Agent-path*/jp1ima/conf/jpc_alertmanager.yml"
--storage.path="data/"	Specify the path where you want to save the administrative data.	N	--	--storage.path="data/alertmanager/"
--data.retention=120h	Specify the retention period for administrative data. Silence information and information about alerts that occurred are saved.	N	--	--data.retention=168h
--alerts.gc-interval=30m	Specifies the interval for the Garbage Collection.	N	--	--alerts.gc-interval=30m
--web.listen-address=":9093"	Specify the listen port. If you want to limit IP address to be listened to, also include Host name or IP address. When Host name is specified, up to 255 bytes can be specified. If you specify Host name or IP address for this option, you must Restart or Prometheus configuration file Prometheus server with the same Host name or IP address for localhost listed in the alerting.alertmanagers.static_configs of Reload (jpc_prometheus_server.yml) alerting.alertmanagers.static_configs on the same host. <Sample Setup> To accept requests for all IP address, you can Setup them as follows: --Web.listen-address=":20714" If you want to limit IP address accepted, you can limit it by specifying Host name or IP address as follows: --Web.listen-address = " Host name or IP address : 20714"	Y	Specify this when you want to change the port or limit the listening IP address.	--web.listen-address=":20714"
--web.get-concurrency=0	Specifies the maximum number of GET requests to process simultaneously.	N	--	--web.get-concurrency=0
--web.timeout=0	Specifies the timeout period for HTTP requests.	N	--	--web.timeout=0
--cluster.listen-address="0.0.0.0:9094"	Specify the listen address when running Alertmanager in HA mode. If you set an empty string, HA mode is disabled.	N	--	--cluster.listen-address=""
--log.level=info	Only messages above the specified level are logged. You can specify one of the following levels: debug, info, warn, or error.	N	Change Setup when you are prompted to change Value from the support desk. Normally, no change is required.	--log.level=info

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--log.format=logfmt	Specifies the output format of log messages. The available output formats are logfmt or json.	N	--	--log.format=logfmt

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- windows_exporter command options

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--telemetry.addr	Specify the listening port. If you want to limit the listening IP address, also include the host name or internet address. If you specify a host name, you can specify up to 255 bytes. If you specify Host name for this option, you must Setup the same Host name as this option to targets of Windows exporter discovery configuration file (jpc_file_sd_config_windows) Windows exporter discovery configuration file on the same host, and Restart or Reload Prometheus server. If you specify IP address for this option, you must Windows exporter discovery configuration file (jpc_file_sd_config_windows) targets on the same host, Setup Host name that resolves to the same IP address as this option and Restart or Reload Prometheus server. <Configuration example> To accept requests for all IP addresses, set the following: --telemetry.addr=":20717" If you want to limit the IP addresses that are accepted, you can specify a host name or an internet address as follows: --telemetry.addr="*host name or IP address*:20717"	Y	Specify this option if you want to change the port or if you want to limit IP address to be listened to.	--telemetry.addr=":20717"
--config.file	Specifies the path to the Windows exporter configuration file. Values set in this file are overwritten by command line options.	Y	--	--config.file="*Agent-path*/jp1ima/conf/jpc_windows_exporter.yml"
--log.level	Only messages above the specified level are logged. You can specify one of the following levels: debug, info, warn, or error.	N	--	--log.level=debug

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- blackbox_exporter command options

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--config.file	Specifies the path to the Blackbox exporter configuration file.	Y	--	--config.file="*Agent-path*/jp1ima/conf/jpc_blackbox_exporter.yml"
--web.listen-address	Specify the listening port. If you want to limit the listening IP address, also include the host name or internet address. If you specify a host name, you can specify up to 255 bytes. If you specify Host name or IP address for this option, you must Setup and Prometheus server Restart or Reload the same Host name or IP address as this option to Prometheus configuration file (jpc_prometheus_server.yml) on the same host in the relabel_config of scrape jobs for blackbox_exporter (more than one). <Configuration example> To accept requests for all IP addresses, set the following: --web.listen-address=":20715" If you want to limit the IP addresses that are accepted, you can specify a host name or an internet address as follows: --web.listen-address="*host name or IP address*:20715"	Y	Specify this when you want to change the port or limit the listening IP address.	--web.listen-address=":20715"
--timeout-offset	Specifies the number of seconds to subtract from the Prometheus scrape_timeout value. The Prometheus scrape_timeout value will now time out in seconds minus the value specified for this option.	N	Offset from timeout period (seconds)	--timeout-offset=0.5
--history.limit	Specifies the upper limit of the history of probe results. This history is stored internally blackbox_exporter, and old history is deleted.	N	Maximum number of items in history	--history.limit=100
--log.level	Only messages above the specified level are logged. You can specify one of the following levels: debug, info, warn, or error.	N	Change Setup when you are prompted to change Value from the support desk. Normally, no change is required.	--log.level=info

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- promitor_scraper command options

  No specifiable options.

- promitor_resource_discovery command options

  No specifiable options.

- script_exporter command options

Item	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
-config.file	Path to configuration file.	Y	--	• For Windows *installation-directory*`\jp1ima\conf\jpc_script_exporter.yml` • For Linux `/opt/jp1ima/conf/jpc_script_exporter.yml`
-web.listen-address	Specifies the standby port. To limit IP addresses for listening, also specify the host name and IP address. Host names up to 255 bytes in length can be specified. Setting example: To receive requests for all IP addresses, configure the following settings as follows: --web.listen-address=":9469" To limit the IP addresses for which requests can be received, specify the host name or IP address as follows: --web.listen-address="*host-name-or-IP-address*:9469"	Y	Specify this to change the port, or to limit IP addresses for listening.	20722
-timeout-offset	Offset to subtract from Prometheus-supplied timeout in seconds. (default 0.5) The system will time out in the sum of the number of seconds specified for this option subtracted from the Prometheus scrape_timeout value.	N	Offset subtracted from the timeout time (seconds)	--timeout-offset=0.5

Legend:

Y: Modifiable, N: Not modifiable, --: Not applicable

- fluentd command options

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
-c	--config.file **PATH**	Specifies configuration file pathname of Fluentd.	Y	For Logical host, you must modify log monitoring common definition file paths that you place in shared folders on Logical host.	Log monitoring common definition file pass of Fluentd
'-i CONFIG_STRING	--enable-input-metrics	Sets the input plug-in metric for Fluentd to Enable.	N	--	None
-G	--conf-encoding **ENCODING**	Specifies the encoding of the configuration File.	N	--	UTF-8

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- oracledb_exporter command-option

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--web.telemetry-path="/metrics"	Specify scrape spacing.	N	--	"/metrics"
--default.metrics="default-metrics.toml"	Specifies the definition file for the default metric.	N	--	"default_metrics.toml"
--custom.metrics=""	Specifies the definition file for the custom metric.	N	--	""
--query.timeout=5	Specifies the timeout period when oracledb_exporter accesses Oracle Database to retrieve information. Specify in hours from 5 to 60. <Setting example> --query.timeout=5	Y	Specify this option when it takes a long time to retrieve data from Oracle Database.	5
--database.maxIdleConns=0	Specifies the maximum number of idle connections.	N	--	1
--database.maxOpenConns=10	Specifies the maximum number of open connections.	N	--	1
--scrape.interval=0s	Specifies the scrape interval.	N	--	0s
--[no-]web.systemd-socket	Specifies if socket-based activation is used.	N	--	Not specified (not used)
--web.listen-address=:9161	Specify the listen port. If you want to limit which IP addresses are listening, also include the hostname or IP address. When a host name is specified, up to 255 bytes can be specified. If you specify a host name or IP address for this option, set the host name or IP address specified as an option to the localhost (There are more than one) listed in the relabel_confg of the scrape job for prometheus.yml oracledb_exporter on the same host, and Prometheus server needs to be restarted or reloaded. <Setting example> To accept a request for all IP addresses, set as follows. --web.listen-address=":20729" If you want to restrict the accepted IP addresses, you can restrict them by hostname or IP addressing as follows: --web.listen-address="hostname or IP address20729"	Y	Specify this when you want to change the port or when you want to limit IP addresses to be listened to.	--web.listen-address="@@port@@"

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--log.level=info	Outputs only messages of the specified level or higher to the log. One of debug, info, warn, error can be specified.	N	Change the setting when the support desk instructs you to change the value. Normally, no change is required.	--log.level=info

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

Unit definition file (jpc_program-name.service)

Format

```
[Unit]
Description = Unit description
After=local-fs.target remote-fs.target rsyslog.service network.target
[Service]
WorkingDirectory = Working directory
ExecStart = /bin/sh -c 'Program Command Line |& (trap "" 15 && exec install
-directory/jp1ima/bin/rotatelogs -n 8#1 log output directory#2 10240K)'
Type = simple
Restart=no
User=root
TimeoutStopSec=Termination timeout period
LimitNOFILE=65536#3
Environment=SIGDUMP_PATH=-#3
[Install]
WantedBy=multi-user.target graphical.target
```

#1

Specify "100" only for unit definition file of Fluentd.

#2

The log-destination directory that is setup as the default value varies depending on the program. For the path of the default value, see *List of files/directories that can be viewed/edited by the user in JP1/IM - Agent of integrated agent host (Linux)* in *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

#3

Described only for unit definition file of Fluentd.

Description

This is a definition file for registering programs in systemctl in the Linux environment.

File

- For a physical host

  `jpc_`*program-name*`.service`

  `jpc_`*program-name*`.service.model` (model file)

- For a logical host

  `jpc_`*program-name_logical-host-name*`.service`

Storage directory

■Integrated agent host

- For a physical host (Model File storage destination)

  `/opt/jp1ima/conf/`

- For Physical host and Logical host (storage destination of definition file)

  `/usr/lib/systemd/system/`

The target of the installation is as follows:

Target name	Description
multi-user.target	runlevel=3 Multi-user mode (text login)
graphical.target	runlevel=5 Multi-user mode (graphical login)

Character code

UTF-8 (without BOM)

Line feed code

LF

When the definitions are applied

It is reflected when you run the systemctl daemon-reload command.

Information that is specified

The startup order of the services on which the Prometheus server, Alertmanager, and Exporter depend is shown below.

- For Prometheus server

Startup order of dependent services	Description
local-fs.target	Local File System
remote-fs.target	Remote File System
rsyslog.service	rsyslog

- For Exporter, and Alertmanager, Fluentd, imagent, imagentproxy, imagentaction

Startup order of dependent services	Description
local-fs.target	Local File System
remote-fs.target	Remote File System
rsyslog.service	rsyslog
network.target	Network

The ending timeout period is shown below.

Types of programs	End timeout period (in seconds)
Prometheus server	110
Alertmanager	60
Node exporter	
Blackbox exporter	
Yet another cloudwatch exporter	
process_exporter	

Types of programs	End timeout period (in seconds)
promitor_scraper	
promitor_resource_discovery	
script_exporter	
Fluentd	
OracleDB exporter	
imagent	140
imagentproxy	
imagentaction	60

The following are the areas that you can change:

- If you want to change command line options

  Edit ExecStart line.

  ■For Prometheus server

  For the parameters of prometheus command, see the description of prometheus command options in *Service definition file (jpc_program-name_service.xml)*.

  ■For Alertmanager

  For the parameters of alertmanager command, see the description of prometheus command options in *Service definition file (jpc_program-name_service.xml)*.

  ■For Node exporter for AIX

  For the arguments of the Node exporter command, see the description of "node_exporter command options" below.

  ■For Node exporter

  About arguments of the node_exporter command, see *node_exporter command options*.

  ■For Yet another cloudwatch exporter

  About arguments of the yet-another-cloudwatch-exporter command, see *yet-another-cloudwatch-exporter command options*.

  ■For Process exporter

  For the parameters of process exporter command, see the description of process_exporter command options in *Process exporter configuration file (jpc_process_exporter.yml)*.

  ■For Primitor

  No specifiable options for the promitor_scraper command and promitor_resource_discovery command.

  ■For Script exporter

  For the parameters of script exporter command, see the description of script exporter command options in *Service definition file (jpc_program-name_service.xml)*.

  ■For OracleDB exporter

  For the arguments of oracledb_exporter command, see the description of oracledb_exporter command options in Service definition file (jpc_program-name_service.xml).

- To change the number of log sectors

  Edit the value after the -n option on the ExecStart line. The number of log sectors that can be specified is 8 to 512.

- To change log size

  Edit the value at the end of the ExecStart line.

- If you want to change the log output destination

Edit the log output directory specified by the rotatelogs argument.

- If you want the process to be restarted automatically when it stops abnormally, specify "always" for Restart. If the process is not restarted automatically, such as in a cluster configuration, specify "no" for Restart.

The options for the node_exporter command and the yet-another-cloudwatch-exporter command are shown below.

- node_exporter command options

  Items related to collectors can be enabled with the "--collector.*collector name*" flag. To invalidate entries for collectors, specify the "--no-collector.*collector name*" flag.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--collector.cpu.info	Enable the collection of node_cpu_info metrics. Specify the ,--collector.cpu.info if you want to enable it. Specify the ,--no-collector.cpu.info if you want to disable it.	Y	--	--collector.cpu.info
--collector.filesystem.ignored-mount-points	Specifies the regular expression for mount points to ignore in the FileSystem collector.	Y	Regular expressions for mount points to ignore in the FileSystem collector	--collector.filesystem.ignored-mount-points="^/(dev|proc|sys|var/lib/docker/.+)($|/)"
--collector.filesystem.ignored-fs-types	Specifies a regular expression for file system types to be ignored by the FileSystem collector.	Y	Regular expressions for mount points to ignore in the FileSystem collector	--collector.filesystem.ignored-fs-types="^/(dev|proc|sys|var/lib/docker/.+)($|/)"
--collector.netstat.fields	Specifies the regular expression for the field to return to the netstat collector.	Y	Regular expression for fields to return to the netstat collector	--collector.netstat.fields="^(.*_(InErrors|InErrs)|Ip_Forwarding|Ip(6|Ext)_(InOctets|OutOctets)|Icmp6?_(InMsgs|OutMsgs)|TcpExt_(Listen.*|Syncookies.*|TCPSynRetrans)|Tcp_(ActiveOpens|InSegs|OutSegs|OutRsts|PassiveOpens|RetransSegs|CurrEstab)|Udp6?_(InDatagrams|OutDatagrams|NoPorts|RcvbufErrors|SndbufErrors))$"
--path.procfs	Specifies the procfs mount point.	Y	The procfs mount point	--path.procfs="/proc"
--path.sysfs	Specifies the sysfs mount point.	Y	The sysfs mount point	--path.sysfs="/sys"
--path.rootfs	Specifies the rootfs mount point.	Y	The rootfs mount point	--path.rootfs="/"
--collector.systemd.unit-include	Specify the unit filename of Systemd to be monitored by the service monitoring function in regular expressions.	Y	Regular expression that matches the unit file name	--collector.systemd.unit-include=""

Item	Description	Ch ang eab ility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	The default is an empty character and no service is monitored. If the regular expressions are incorrect, Node exporter fails to start servicing. Depending on how the regular expression is specified, it may take time to collect performance information. For more information, see *Appendix G.4 Tips on using regular expressions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.			
--collector.cpu	Enable the cpu collector. If enabled,-- specify collector.cpu. If you want to disable it,-- specify no-collector.cpu.	Y	--	--collector.cpu
--collector.diskstats	Enable the diskstats collector. If enabled,-- specify collector.diskstats. To disable it,-- specify no-collector.diskstats.	Y	--	--collector.diskstats
--collector.filesystem	Enable the FileSystem collector. If enabled,-- specify collector.filesystem. If disabled,-- specify no-collector.filesystem.	Y	--	--collector.filesystem
--collector.loadavg	Enable the loadavg collector. If enabled,-- specify collector.loadavg. If you want to disable it,-- specify no-collector.loadavg.	Y	--	--collector.loadavg
--collector.meminfo	Enable the meminfo collector. If enabled,-- specify collector.meminfo. To disable it,-- specify no-collector.meminfo.	Y	--	--collector.meminfo
--collector.netclass	Enable the netclass collector. If enabled,-- specify collector.netclass. If disabled,-- specify no-collector.netclass.	Y	--	--collector.netclass
--collector.netdev	Enable the netdev collector. If enabled,-- specify collector.netdev. If disabled,-- specify no-collector.netdev.	Y	--	--collector.netdev
--collector.netstat	Enable the netstat collector. If enabled,-- specify collector.netstat. To disable it,-- specify no-collector.netstat.	Y	--	--collector.netstat
--collector.nfs	Enable the nfs collector. If enabled,-- specify collector.nfs. To disable it,-- specify no-collector.nfs.	Y	--	--collector.nfs

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
--collector.nfsd	Enable the nfsd collector. If enabled,-- specify collector.nfsd. To disable it,-- specify no-collector.nfsd.	Y	--	--collector.nfsd
--collector.stat	Enable the stat collector. If enabled,-- specify collector.stat. To disable it,-- specify no-collector.stat.	Y	--	--collector.stat
--collector.systemd	Enable systemd collector. When enabled, specifies --collector.systemd. When disabled, specifies --nocollector.systemd.	Y	--	--collector.systemd
--collector.time	Enable the time collector. If enabled,-- specify collector.time. To disable it,-- specify no-collector.time.	Y	--	--collector.time
--collector.uname	Enable the uname collector. If enabled,-- specify collector.uname. To disable it,-- specify no-collector.uname.	Y	--	--collector.uname
--collector.vmstat	Enable the vmstat collector. If enabled,-- specify collector.vmstat. To disable it,-- specify no-collector.vmstat.	Y	--	--collector.vmstat
--web.listen-address	Specify the listening port. If you want to limit the listening IP address, also include the host name or internet address. If you specify a host name, you can specify up to 255 bytes. If a host name is specified for this option, the targets of the Node exporter's discovery configuration file (jpc_file_sd_config_node.yml) on the same host must be set to the same host name as this option, and the Prometheus server must be restarted or reloaded. If an internet address is specified for this option, the targets of the Node exporter's discovery configuration file (jpc_file_sd_config_node.yml) on the same host must be set to a host name that resolves to the same IP address as this option, and the Prometheus server must be restarted or reloaded. <Configuration Example> To accept requests for all IP addresses, set the following: --web.listen-address=":20716" If you want to limit the IP addresses that are accepted, you can specify a host name or an internet address as follows:	Y	Specify this when you want to change the port or limit the listening IP address.	--web.listen-address=":20716"

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	--web.listen-address="*hostname or IP address*: 20716"			
--web.max-requests	Specifies the maximum number of scrape requests to accept at the same time.	N	--	--web.max-requests=40
--log.level=info	Only messages above the specified level are logged. You can specify one of the following levels: debug, info, warn, or error.	N	Change Setup when you are prompted to change Value from the support desk. Normally, no change is required.	--log.level=debug

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

- yet-another-cloudwatch-exporter command options

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
-cloudwatch-concurrency	Specify the maximum number of concurrent requests to the Amazon CloudWatch API.	Y	Maximum concurrent requests	-cloudwatch-concurrency=5
-config.file	Specify the path to the Yet another cloudwatch exporter configuration file.	Y	--	-config.file="*Agent-path*/jp1ima/conf/jpc_ya_cloudwatch_exporter.yml"
-fips	Specify this in when using API of FIPS compliant Amazon Web Services (AWS)#. #: This should be specified, for example, if your security requirements require compliance with Federal Information Processing Standard (FIPS) 140-2).	Y	Specify if you want to enable it.	Do not specify (do not enable)
-listen-address	Specify the listening port. If you want to limit the listening IP address, also include the host name or internet address. If you specify a host name, you can specify up to 255 bytes. If you specify Host name for this option, you must Setup the same Host name as this option to targets of Yet another cloudwatch exporter discovery configuration file (jpc_file_sd_config_cloudwatch.yml) Yet another cloudwatch exporter discovery configuration file on the same host, and Restart or Reload Prometheus server. If you specify IP address for this option, you must Yet another cloudwatch exporter discovery configuration file (jpc_file_sd_config_cloudwatch.yml) targets on the same host, Setup Host name that resolves to	Y	Specify this when you want to change the port or limit the listening IP address.	-listen-address=":20718"

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	the same IP address as this option and Restart or Reload Prometheus server. <Configuration Example> To accept requests for all IP addresses, set the following: -listen-address=":20718" If you want to limit the IP addresses that are accepted, you can specify a host name or an internet address as follows: -listen-address="*hostname or IP address*:20718"			
-metrics-per-query	Specifies the number of metrics created in a single GetMetricsData request.	Y	Normally, you don't change it.	-metrics-per-query=500
-tag-concurrency	Specifies the maximum number of concurrent requests to the Resource Tagging API.	Y	Normally, you don't change it.	-tag-concurrency=5

Legend:

Y: Changeable, --: Not applicable

Windows exporter configuration file (jpc_windows_exporter.yml)

Format

Write in YAML format.

```
collectors:
  enabled: cache,cpu,logical_disk,memory,net,system,cs,process,service#
collector:
  logical_disk:
    volume-whitelist: ".+"
    volume-blacklist: ""
  net:
    nic-whitelist: ".+"
    nic-blacklist: ""
  process:
    process-whitelist: ""
    process-blacklist: ""
  service:#
    services-where: "Name=''"
scrape:
  timeout-margin: 0.5
```

#

Parameters for service monitoring that are set in the model file by JP1/IM - Agent 13-01 or later installer.

If you want to use the service monitoring feature by upgrading from JP1/IM - Agent 13-00 to 13-01 or later, you can manually set and edit the service monitoring parameters. For details, see the instructions for configuring service monitoring in *1.21.2(5)(b) Modify metric to Collect (Optional)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

File

`jpc_windows_exporter.yml`

`jpc_windows_exporter.yml.model` (model file)

Storage directory

■Integrated agent host

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

Description

This is a configuration file that specifies the operation of Windows exporter.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

It will take effect when you restart Windows exporter.

Information that is specified

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
collectors	--	--	--	--
enabled	Specify the collectors to use, separated by commas.	• For 13-00 N • For 13-01 or later Y	--	• For 13-00 collectors: enabled:cache,cpu,logical_disk,memory,net,system,cs,process • For 13-01 or later collectors: enabled:cache,cpu,logical_disk,memory,net,system,cs,process,service
dfsr	--	--	--	--
exchange	--	--	--	--
mssql	--	--	--	--
collector	--	--	--	--
iis	--	--	--	--
logical_disk	--	--	--	--
volume-whitelist	Set the volume to be collected using a regular expression. Volumes that fall into both volume-whitelist and volume-blacklist are not collected (volume-blacklist takes precedence).	Y	Specify the volume to the whitelist with a regular expression.	collector: logical_disk: volume-whitelist: ".+"
volume-blacklist	Set the volumes not to be collected by regular expression. Volumes that fall into both volume-whitelist and volume-blacklist are not collected (volume-blacklist takes precedence).	Y	Specify the volume to the blacklist with a regular expression.	collector: logical_disk: volume-blacklist: ""
msmq	--	--	--	--
net	--	--	--	--
nic-whitelist	Set the NICs to be collected using regular expressions. NICs that fall into both nic-whitelist and nic-blacklist are not collected (nic-blacklist takes precedence).	Y	Specify the NICs to the whitelist as a regular expression.	collector: net: nic-whitelist: ".+"

Item			Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value

			The name of the NIC specified in this item must be the value obtained by the following command.
			`wmic path Win32_PerfRawData_Tcpip_NetworkInterface get name`
			Note that this item is treated as a regular expression, so if you want to specify a special character of the regular expression, you need to escape it with a backslash. In this case, the backslash is treated as a special character in YAML, so it is necessary to write the backslash twice.
			(Example description)
			If you want to specify "Intel[R] Dual Band Wireless-AC 8265" as an exact match
			`nic-whitelist: "Intel\\[R\\] Dual Band Wireless-AC 8265"`			

		nic-blacklist	Set the NICs not to be collected using regular expressions. NICs that fall into both nic-whitelist and nic-blacklist are not collected (nic-blacklist takes precedence). This entry is specified in the same way as nic-whitelist.	Y	Specify the NICs to the blacklist with regular expressions.	collector: net: nic-blacklist: ""
	process		--	--	--	--
		whitelist	Regexp of volumes to whitelist. Volume name must both match whitelist and not match blacklist to be included. If omitted, this is specified as ".+".	Y	--	collector: process: whitelist: ""
		blacklist	Regexp of volumes to blacklist. Volume name must both match whitelist and not match blacklist to be included. If omitted, this is specified as "".	Y	--	collector: process: blacklist: ""
	service		--	--	--	--
	services-where		Specifies 'where' phrase for WQL to use in WMI metric queries. (Example of specification when monitoring multiple services) services-where: "Name='jpc_imagent' OR Name='jpc_imagentproxy' OR Name='jpc_imagentaction'" #	Y	Specifies the service name to monitor.	services-where: "Name=''"

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
		If an invalid character string is specified, the service is not monitored. For details about the log output, see *12.5.1(4) node_exporter log* in the *JP1/ Integrated Management 3 - Manager Administration Guide*.			
	smtp	--	--	--	--
	textfile	--	--	--	--
log		--	--	--	--
scrape		--	--	--	--
	timeout-margin	Specifies the number of seconds to subtract from the Prometheus scrape_timeout value (specify a value that is less than the Prometheus scrape_timeout value). It will time out in seconds after subtracting the value specified for this item from the value of the Prometheus scrape_timeout. For Prometheus scrape_timeout values, see the *scrape_timeout* in *Information that is specified* of *Prometheus configuration file (jpc_prometheus_server.yml)*.	Y	Tolerance for overhead or high load is usually not required. Use to tune to allow for overhead or high load.	scrape: timeout-margin: 0.5

Legend:

Y: Changeable, N: Not changeable, --: Not applicable

Process exporter configuration file (jpc_process_exporter.yml)

Syntax

Written in YAML format.

```
process_names:
  - name: "{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}"
    cmdline:
    - (?P<cmdline>.*)
```

File

`jpc_process_exporter.yml`

`jpc_process_exporter.yml.model` (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\`

When using a logical host

shared-folder`\jp1ima\conf\`

For Linux

When using a physical host

`/opt/jp1ima/conf/`

When using a logical host

shared-directory`/jp1ima/conf/`

Description

The configuration file that determines the behavior of Process exporter.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

When Process exporter is restarted.

Content description

Item#			Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
process_names			--	--	--	--
-	[name]		Each item in process_names gives a recipe for identifying and naming processes. The optional name tag defines a template to use to name matching processes; if not specified, name defaults to `{{.ExeBase}}`. • `{{.Comm}}` contains the basename of the original executable, i.e. 2nd field in `/proc/<pid>/stat` • `{{.ExeBase}}` contains the basename of the executable • `{{.ExeFull}}`contains the fully qualified path of the executable • `{{.Username}}` contains the username of the effective user • `{{.Matches}}` map contains all the matches resulting from applying cmdline regexps • `{{.PID}}` contains the PID of the process. Note that using PID means the group will only contain a single process. • `{{.StartTime}}` contains the start time of the process. This can be useful in conjunction with PID because PIDs get reused over time. • `{{.Cgroups}}` contains (if supported) the cgroups of the process (/proc/self/cgroup). This is particularly useful for identifying to which container a process belongs.	Y	Specify this to change the process name to a value other than the default value (executable file name).	{{.ExeBase}};{{.Username}};{{.Matches.cmdline}}
	<selector>		comm, exe or cmdline. If more than one selector is present, they must all match.	REQ	Monitored process selector	cmdline
	-	<any>	For "`comm`" and "`exe`", the list of strings is an OR, meaning any process matching any of the strings will be added to the item's group. For "`cmdline`", the list of regexes is an AND, meaning they all must match. Any capturing groups in a regexp must use the `?P<name>` option to assign a name to the capture, which is used to populate "`.Matches`". • `comm` `comm` is the second field of `/proc/<pid>/stat` minus parens. It is the base executable name, truncated at 15 chars. It cannot be modified by the program, unlike `exe`. ex) `bash` • `exe` `exe` is `argv[0]`. If no slashes, only basename of `argv[0]` need match. If exe contains slashes, `argv[0]` must match exactly.	REQ	Monitored process selector value	- (?P<cmdline>.*)

Item#	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent

	ex) `/usr/local/bin/prometheus`
	- `cmdline`
	`cmdline` is a list of regexps applied to argv. Each must match, and any captures are added to the ".Matches" map.
	Specify this within 4,096 bytes.
	For details on the process_exporter arguments, see *process_exporter command options*.
	ex)
	`- name: "{{.ExeFull}}:{{.Matches.Cfgfile}}"`
	`exe:`
	`- /usr/local/bin/process-exporter`
	`cmdline:`
	`- -config.path\s+(?P<Cfgfile>\S+)`			

Legend:

REQ: Required setting, Y: Modifiable, --: Not applicable

#

Brackets (`[]`) denote optional items.

- process_exporter command options

Item	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
-web.listen-address	Address on which to expose metrics and web interface. If omitted, this is specified as :9256.	Y	Specify this to change the port, or to limit IP addresses for listening.	20721
-procnames	comma-separated list of process names to monitor Specify the `comm` field value in `/proc//stat` as the process name. Process names cut off at 15 characters.	Y	--	None
-procfs	path to read proc data from If omitted, this is specified as `/proc`.	Y	--	None
-namemapping	comma-separated list, alternating process name and capturing regex to apply to cmdline Renamed names that are not in the procnames list are ignored. Setting example: `-namemapping "python2,([^/]+).py,java,-jar\s+([^/]+).jar"`	Y	--	None
-config.path	path to YAML config file	Y	--	*installation-directory*`/jp1ima/conf/`

Item	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
				`jpc_process_exporter.yml`

Legend:

Y: Modifiable, --: Not applicable

Blackbox exporter configuration file (jpc_blackbox_exporter.yml)

Format

Write in YAML format.

```
modules:
  http:
    prober: http
    http:
      method: GET
      compression: ""
      follow_redirects: true
      fail_if_ssl: false
      fail_if_not_ssl: false
      preferred_ip_protocol: ip4
      ip_protocol_fallback: false
      body: ""
      tls_config:
        insecure_skip_verify: true
  icmp:
    prober: icmp
    icmp:
      preferred_ip_protocol: ip4
      ip_protocol_fallback: false
```

File

`jpc_blackbox_exporter.yml`

`jpc_blackbox_exporter.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

■Integrated manager host (model File only)

`/opt/jp1pccspkg/jp1_pc_agent_probe/jp1_pc_agent_probe_windows_`*JP1/IM - Agent-version-number-(VVRRSS-format)*`/blackbox_exporter/conf/`

`/opt/jp1pccspkg/jp1_pc_agent_probe/jp1_pc_agent_probe_linux_`*JP1/IM - Agent-version-number-(VVRRSS-format)*`/blackbox_exporter/conf/`

■Monitoring agent host

In Windows:

- For a physical host
  Install the monitoring agent directory`\jp1pccs\conf\`
- For a logical host
  shared-directory`\jp1pccs\conf\`

In Linux:

- For a physical host
  Install the monitoring agent directory`/jp1pccs/conf/`
- For a logical host
  shared-directory`/jp1pccs/conf/`

Description

A configuration file that specifies the operation of the Blackbox exporter.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflected when the Blackbox exporter is restarted or when the Blackbox exporter reload API is executed.

Information that is specified

For definitions of common placeholders used in the table below, see *About definition of common placeholders for descriptive items in yml file*.

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Modules		--	Y	--	--
	module_name	Specify a module name of your choice. Specify this if you want to create a module with different settings from the one you have already created. When you create a module, you must also create a scrape definition and a discovery configuration file. For setup instructions, see *1.21.2(6) Setup of Blackbox exporter* and *1.21.2(3)(c) Add Blackbox exporter scrape job (for Windows) (optional)* for Windows and *2.19.2(7) Setup of Blackbox exporter* and *2.19.2(3)(c) Add a Blackbox exporter scrape job (for Linux) (optional)* for Linux in the *JP1/Integrated Management 3 - Manager Configuration Guide*.	Y	--	For the modules to be defined as the default setup, see *1.21.2(6) Setup of Blackbox exporter* and *2.19.2(7) Setup of Blackbox exporter* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Item				Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
				When monitoring is performed with a created module, there is no need to define a new `module_name`, and the information to be monitored is added to the `targets` of the created discovery configuration file. <Configuration Example> modules: http_2xx:			
		prober: <prober_string>		Specifies the protocol to probe. You can specify `http` or `icmp`.	Y	Specify `http` or `icmp`.	None
		[http: <http_probe>]		Configure the http protocol settings. For details, see <http_probe> below.	Y	Specifies parameters for a specific protocol.	Not specified
		[icmp: <icmp_probe>]		Configure the icmp protocol settings. For details, see <icmp_probe> below.	Y	Specifies parameters for a specific protocol.	Not specified
		<http_probe>		--	--	--	--
			[valid_status_codes: <int>, ...]	Specify acceptable HTTP status codes. If the specification is omitted or an empty value is specified, the 200 series is allowed. <Configuration Example> valid_status_codes: [200, 201]	Y	Specify when status codes other than the 200 series are treated as normal.	Not specified
			[valid_http_versions: <string>, ...]	Specify the allowed HTTP versions. If omitted or empty is specified, all are allowed. <Configuration Example> valid_http_versions: ["HTTP/1.1", "HTTP/2"]	Y	Specify this when you want to limit the allowed HTTP versions.	Not specified
			[method: <string>]	Specify the HTTP method to use. <Configuration Example> method: GET	Y	Specify the HTTP method to use.	GET
			headers: [<string>: <string> ...]	Specify the headers of the HTTP request. If the `Accept-Encoding` header is specified, see also the item on `compression`. <Configuration Example> headers: Host: host.example.com Accept-Language: en-US	Y	Specify the headers of the HTTP request.	Not specified
			[compression: <string>]	Specifies the compression algorithm to use to decompress the response. You can specify `gzip`, `br`, `deflate`, `identity`. If the `Accept-Encoding` header is specified, the compression algorithm specified with this option must be allowed.	Y	Specifies the compression algorithm to use.	""
			[follow_redirects: <boolean>]	Specifies whether HTTP redirects should be followed. You can specify `true` or `false`.	Y	Specify true to enable.	true
			[fail_if_ssl: <boolean>]	Specifies whether the probe fails when SSL is presented.	Y	Specify true to enable.	false

Item					Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
					You can specify `true` or `false`.			
			[fail_if_not_ssl: <boolean>]		Specifies whether SSL should fail if not presented. You can specify `true` or `false`.	Y	Specify true to enable.	false
			fail_if_body_matches_regexp:[- <regex>, ...]		Specifies a regular expression to be treated as invalid if it matches the response body. If the response body matches the regular expression, the probe fails. Multibyte characters are not allowed. <Configuration Example> fail_if_body_matches_regexp: - "Could not connect to database"	Y	Specifies if you want the probe to fail depending on the contents of the response body.	Not specified
			fail_if_body_not_matches_regexp:[- <regex>, ...]		Specifies a regular expression to be treated as invalid if it does not match the response body. If the response body does not match the regular expression, the probe fails. Multibyte characters are not allowed. <Configuration Example> fail_if_body_not_matches_regexp: - "Download the latest version here"	Y	Specifies if you want the probe to fail depending on the contents of the response body.	Not specified
			fail_if_header_matches:[- <http_header_match_spec>, ...]		Specify a regular expression to be treated as invalid when it matches the response header. If the response header matches the regular expression, the probe fails. Headers with multiple values are treated as failed if at least one matches. For details, see *<http_header_match_spec>* below.	Y	Specify if you want the probe to fail based on the contents of the response header.	Not specified
			fail_if_header_not_matches:[- <http_header_match_spec>, ...]		Specify a regular expression to be treated as invalid if it does not match the response header. If the response header does not match the regular expression, the probe fails. Headers with multiple values are treated as failed if they do not match all of them. For details, see *<http_header_match_spec>* below.	Y	Specify if you want the probe to fail based on the contents of the response header.	Not specified
			tls_config: [<tls_config>]		Sets the TLS protocol configuration for the HTTP probe. For details, see <tls_config> below.	Y	For details, see <tls_config> below.	Specify the following values: insecure_skip_verify: true
			basic_auth:		Set the HTTP basic authentication credentials for the target.	Y	--	None
				[username: <string>]	Specifies User name for accessing the target. Password must be Add using the Secret Management command.	Y	Specify for Basic authentication.	None
			[proxy_url: <string>]		Specifies HTTP proxy server to use to connect to the monitoring target. Format: http://host-name-or-IP-address:port-number	Y	Required to connect to the monitoring target through a proxy server.	None

Item				Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
			[skip_resolve_phase_with_proxy: <boolean>]	In the case that HTTP proxy (proxy_url) is specified, when you skip DNS resolution and change of URL performed by Blackbox exporter, set `true`, when you do not skip them, set `false`. For example, in the case that target is https://www.example.com:1234 and goes through proxy, Blackbox exporter tries to go through proxy using https://123.45.67.8:1234 due to DNS resolution and change of URL, when proxy allows only https://www.example.com:1234 then connection to target is unavailable, it is enabled by setting `true`. If omitted, it is treated as `false`.	Y	In the case that HTTP proxy (proxy_url) is specified, when you skip DNS resolution and change of URL performed by Blackbox exporter, set `true`, when you do not skip them, set `false`.	None
			[proxy_user: <string>]	Specify user name if HTTP proxy server that you want to use to connect to the target requires Basic authentication. For user name, specify a user name that does not URL encode. Password must be add using the secret management command.	Y	Required if you are going through a proxy server with authentication to connect to the target.	None
			[preferred_ip_protocol: <string>]	Specifies the preferred protocol. Only `ip4` can be specified.	R	Specify ip4.	None
			[ip_protocol_fallback: <boolean>]	Specifies whether to retreat if the preferred protocol is not available. Only `false` can be specified.	R	Specify false.	None
			body: [<string>]	Specifies the body of the HTTP request used by the probe.	R	Specifies the body of the HTTP request used by the probe.	""
		<http_header_match_spec>		--	--	--	--

			header: <string>,	Specify the header field name.
				<Configuration Example>
				`fail_if_header_matches: # Verifies that no cookies are set`
				`  - header: Set-Cookie`
				`    allow_missing: true`
				`    regexp: '.*'`
					R	Specify the header field name.	None

			regexp: <regex>,	Specifies the comparison string (regular expression). Multibyte characters are not allowed.	R	Specifies the comparison string (regular expression).	None
			[allow_missing: <boolean>]	Specifies whether the absence of a header field is allowed.	Y	Specify true to enable.	false
		<icmp_probe>		--	--	--	--
			[preferred_ip_protocol: <string>]	Specifies the preferred protocol. Only `ip4` can be specified.	R	Specify ip4.	--
			[ip_protocol_fallback: <boolean>]	Specifies whether to retreat if the preferred protocol is not available. Only `false` can be specified.	R	Specify false.	--

Item				Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
			[source_ip_address: <string>]	Specify the source IP address.	Y	Specify to fix the source IP address.	Not specified
			[dont_fragment: <boolean>]	Specifies the DF bit of the IP header. You can specify `true` or `false`. It only works with `ip4`.	Y	Specifies that fragments should not be made.	Not specified
		<tls_config>		--	--	--	--
			[insecure_skip_verify: <boolean>]	Specifies whether to disable certificate validation for the target. You can specify `true` or `false`. If you want to monitor the following metrics, you must specify `false`, place the certificate, and specify the path of the certificate file in the appropriate parameters: Also, if you specify `true`, the values of the following metrics will not be correct. • probe_ssl_last_chain_expiry_timestamp_seconds If an IP address is specified instead of a host name in the `targets` URL of the discovery configuration file (jpc_file_sd_config_blackbox_http.yml) of Blackbox exporter (HTTP/HTTPS monitoring), `false` cannot be specified.	Y	Specify true to disable validation; false to enable.	• For http modules true • In cases other than the above Not specified
			[ca_file: <filename>]	Specifies the CA certificate to use for the target. Is. If the `Insecure_skip_verify` parameter is `false`, it is required. Place the file under the following directory and specify the path to the file: • In Linux: *installation-directory*`/jp1ima/conf/user/cert/` • In Windows: *installation-directory*`\jp1ima\conf\user\cert\` For details, see *List of files/directories that can be view ed/edited by the user in JP1/IM - Agent of integrated agent host* on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.	Y	Specify the CA certificate file.	Not specified
			[cert_file: <filename>]	Specifies the client certificate file for the target. Required if the monitored target requires client authentication. Place the file under the following directory and specify the path to the file: • In Linux: *installation-directory*`/jp1ima/conf/user/cert/` • In Windows:	Y	Specifies the client certificate file.	--

Item				Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
				installation-directory`\jp1ima\conf\user/cert\` For details, see *List of files/directories that can be view ed/edited by the user in JP1/IM - Agent of integrated agent host* on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.			
			[key_file: <filename>]	Specify the client certificate key file for the target. Required if the monitored target requires client authentication. Place the file under the following directory and specify the path to the file: • In Linux: *installation-directory*`/jp1ima/conf/user/secret/` • In Windows: *installation-directory*`\jp1ima\conf\user\secret\` For details, see *List of files/directories that can be view ed/edited by the user in JP1/IM - Agent of integrated agent host* on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.	Y	Specifies the client certificate key file.	--
			[server_name: <string>]	Specifies the server name used to verify the hostname of the target.	Y	Specify the server name.	Host name of the target host

Legend:

R: Required, Y: Changeable, --: Not applicable

Yet another cloudwatch exporter configuration file (jpc_ya_cloudwatch_exporter.yml)

Format

Write in YAML format.

```
discovery:
  exportedTagsOnMetrics:
    AWS/EC2:
      - jp1_pc_nodelabel
    AWS/Lambda:
      - jp1_pc_nodelabel
    AWS/S3:
      - jp1_pc_nodelabel
    AWS/DynamoDB:
      - jp1_pc_nodelabel
    AWS/States:
      - jp1_pc_nodelabel
    AWS/SQS:
      - jp1_pc_nodelabel
    AWS/ESC:
      - jp1_pc_nodelabel
    AWS/EBS:
      - jp1_pc_nodelabel
    AWS/EFS:
      - jp1_pc_nodelabel
    AWS/FSx:
      - jp1_pc_nodelabel
    AWS/SNS:
      - jp1_pc_nodelabel
    AWS/RDS:
      - jp1_pc_nodelabel
  jobs:
  - type: AWS/EC2
    regions:
      - ap-northeast-1
    period: 0
    length: 600
    delay: 120
    metrics:
      - name: CPUUtilization
        statistics:
        - Average
      - name: DiskReadBytes
        statistics:
        - Sum
      - name: DiskWriteBytes
        statistics:
        - Sum
```

File

`jpc_ya_cloudwatch_exporter.yml`

`jpc_ya_cloudwatch_exporter.yml.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

■Integrated manager host (model File only)

`/opt/jp1pccspkg/jp1_pc_agent_cloud/jp1_pc_agent_cloud_linux_`*JP1/IM - Agent-version-number-(VVRRSS-format)*`/ya_cloudwatch_exporter/conf/`

■Monitoring agent host

- For a physical host
  Install the monitoring agent directory`/jp1pccs/conf/`
- For a logical host
  shared-directory`/jp1pccs/conf/`

Description

A configuration file that specifies the behavior of Yet another cloudwatch exporter.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When you restart Yet another cloudwatch exporter, it will be reflected in the behavior of Yet another cloudwatch exporter.

Also, when you execute the jddcreatetree command and the jddupdatetree command after performing the above operation, it is reflected in the displayed contents of the tree in the integrated operation viewer.

Information that is specified

- Top-level parameters
  The discovery listed in the following table is listed.

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
discovery	Configure Auto-discovery. For more information, see <Auto-discovery configuration> below.	Y	See <Auto-discovery configuration>.	None

Legend:

Y: Changeable

- <Auto-discovery configuration>

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
<Auto-discovery configuration>		--	--	--	--
	exportedTagsOnMetrics	Specifies a list of tags per service to export to all metrics. Be sure to specify the jp1_pc_nodelabel tag. <Example List> exportedTagsOnMetrics: AWS/EC2: - jp1_pc_nodelabel - type Precautions Only tagged AWS resources are discovered.	Y	List of tags per service to export to all metrics	exportedTagsOnMetrics: AWS/EC2: - jp1_pc_nodelabel AWS/Lambda: - jp1_pc_nodelabel AWS/S3: - jp1_pc_nodelabel AWS/DynamoDB: - jp1_pc_nodelabel AWS/States: - jp1_pc_nodelabel AWS/SQS: - jp1_pc_nodelabel AWS/EBS: - jp1_pc_nodelabel AWS/ECS: - jp1_pc_nodelabel AWS/EFS: - jp1_pc_nodelabel AWS/FSx: - jp1_pc_nodelabel AWS/RDS: - jp1_pc_nodelabel AWS/SNS: - jp1_pc_nodelabel ECS/ContainerInsights: - jp1_pc_nodelabel
	jobs	Configure the list of Auto-discovery jobs. See <Auto-discovery job> below.	R	See <Auto-discovery job>.	--

Legend:

R: Required, Y: Changeable, --: Not applicable

- <Auto-discovery job>

Item	Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
<Auto-discovery job>	--	--	--	--
regions	Specify a list of AWS Regions.	R	List of AWS Regions	ap-northeast-1
type	Specify the namespace name, such as "AWS/EC2", "AWS/S3", and so on. For details about the namespaces (services) that can be specified, see the following section of the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. JP1/IM - Agent's Yet another cloudwatch exporter supports AWS namespaces for monitoring in *3.15.6(1)(k) Creating an IM Management Node for Yet another cloudwatch exporter*	R	Namespace name	AWS/EC2 AWS/Lambda AWS/S3 AWS/DynamoDB AWS/States AWS/SQS AWS/EBS AWS/ECS AWS/EFS AWS/FSx AWS/RDS AWS/SNS ECS/ContainerInsights
length	Specifies the duration in seconds for retrieving data from CloudWatch. The acquisition start time is "current time - (length + delay)".	Y	Time to request data (in seconds)	• Non-AWS/S3 settings length: 600 • AWS/S3 settings length: 172800
delay	Specifies the number of seconds in advance to request data for the current time. The acquisition end time is "current time - delay".	Y	--	delay: 120
roles	Specify the IAM role to assume. You can write up to two roles. <Configuration Example> roles: - roleArn: "arn:aws:iam::1111111111111:role/cross_access_role" - roleArn: "arn:aws:iam::2222222222222:role/cross_access_role"	Y	List of IAM Roles to Assume	Not specified
searchTags	Specifies a list of key-value pairs to use (all must match) to use if only data with a particular tag is to be collected. The value can be a regular expression. Do not delete the entries that are set by default. <Configuration Example> searchTags: - key: env value: production	Y	List of key-value pairs	searchTags: - key: jp1_pc_nodelabel value: .*
period	Specifies the granularity of the data retrieved from CloudWatch in seconds.	Y	Statistics period in seconds	0

Item		Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
	customTags	Specifies the custom tag to add as a list of key-value pairs. <Configuration Example> customTags: - key: CustomTag value: CustomValue	Y	Custom Tags	Not specified
	metrics	Configure a list of metric definitions. For more information, see <metric definitions> below.	R	List of metric definitions	Set the metric defined in the initial value of the metric definition file. For the initial values of the metric definition file, see the section explaining *Model file settings (initial state)* in *Yet another cloudwatch exporter metric definition file (metrics_ya_cloudwatch_exporter.conf)*.

Legend:

R: Required, Y: Changeable, --: Not applicable

- <metric definitions>

Item			Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
<metric definitions>			--	--	--	--
		name	Specify the CloudWatch metric name.	R	CloudWatch metric name	None
		statistics	Specifies the statistic type in list format. Specify Minimum, Maximum, and so on. <Configuration Example> statistics: - Average	R	Statistic type	None
		period	Specifies the granularity of the data retrieved from CloudWatch in seconds. This definition overrides the job-level setting.	Y	Statistics period in seconds	• If the <Auto-discovery job> period is 0 300 • If the <Auto-discovery job> period is other than 0 Settings value of period in <Auto-discovery job>
		nilToZero	Specify True to treat 0 when information cannot be retrieved from CloudWatch. The default is False.	Y	Specify True to enable.	Not specified

Legend:

R: Required, Y: Changeable, --: Not applicable

Promitor Scraper configuration file (metrics-declaration.yaml)

Syntax

Written in YAML format.

```
verion: v1
azureMetadata:
  tenantId: tenant-ID
  subscriptionId: subscription-ID
  resourceGroupName: resource-group-name
metricDefaults:
  aggregation:
    interval: 00:05:00
  scraping:
  schedule: "0 * * ? * *"
metrics:
  - name: azure_virtual_machine_disk_read_bytes_total
    description: "Bytes read from disk during monitoring period."
    scraping:
      schedule: "0 * * ? * *"
    azureMetricConfiguration:
      metricName: Disk Read Bytes
      aggregation:
        type: Total
    resourceDiscoveryGroups:
    - name: virtual-machine-group
```

File

`metrics-declaration.yaml`

`metrics-declaration.yaml.model` (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\promitor\scraper\`

When using a logical host

shared-folder`\jp1ima\conf\promitor\scraper\`

For Linux

When using a physical host

`/opt/jp1ima/conf/promitor/scraper/`

When using a logical host

shared-directory`/jp1ima/conf/promitor/scraper/`

Description

The configuration file that defines the metrics to be acquired by the Promitor Scraper.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in Promitor Scraper behavior when restarting Promitor Scraper.

After performing the action above, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

Item#	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
version	Version of declaration that is used. Allowed values are v1.	N	--	v1
azureMetadata:	Azure information	--	--	--
tenantId:	The id of the Azure tenant that will be queried.	REQ	Tenant ID	None
subscriptionId:	The id of the default subscription to query.	REQ	Subscription ID	None
resourceGroupName:	The name of the default resource group to query.	REQ	Resource group name	None
[cloud:]	The name of the Azure cloud to use. Options are Global (default), China, UsGov & Germany.	Y	--	None
metricDefaults:	Metric default settings	--	--	--
aggregation:	Aggregation settings	Y	--	--
[interval]:	The default interval which defines over what period measurements of a metric should be aggregated. a cron that fits your needs.	Y	--	00:05:00
[limit]:	The default maximum amount of resources to scrape when using dimensions or filters. If omitted, this is specified as 10000.	Y	--	None
labels:	The default labels that will be applied to all metrics.	--	--	--
<key>: <value>	Specify the key and value in a character string of 1 to 255 characters. The key value must be specified with characters that match the regular expression [a-z _:][a-z0-9_:]*. Multibyte characters can not be specified for the value.	Y	--	None

Item#			Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
	scraping:		scraping settings	--	--	--
		schedule:	A cron expression that controls the frequency of which all the configured metrics will be scraped from Azure Monitor. You can use crontab-generator.org to generate a cron that fits your needs. Setting example: If the schedule is set to every minute `0 * * ? * *`	Y	--	"0 * * ? * *" The Promitor setting example, and the default collection interval for Prometheus and Azure Monitor provided by JP1/IM - Agent are one minute.
metrics:			metrics settings	--	--	--
-	name:		Name of the metric that will be reported. Specify in a character string of 1 to 255 characters. The value must be specified with characters that match the regular expression [a-zA-Z_:][a-zA-Z0-9_:]*.	Y	--	Varies depending on the metric.
	description:		Description for the metric that will be reported. Specify using 1 to 255 characters, excluding control characters.	Y	--	Varies depending on the metric.
	resourceType:		Defines what type of resource needs to be queried. The following shows values that can be specified: • VirtualMachine • FunctionApp • ContainerInstance • KubernetesService • FileStorage • BlobStorage • ServiceBusNamespace • CosmosDb • SqlDatabase • SqlManagedInstane • SqlElasticPool • LogicApp	Y	--	Varies depending on the metric.
	[labels:]		Defines a set of custom labels to include for a given metric.	--	--	--
		<key>: <value>	Specify the key and value in a character string of 1 to 255 characters. The key value must be specified with characters that match the regular expression [a-z _:][a-z0-9_:]*. Multibyte characters can not be specified for the value.	Y	--	None
	[scraping:]		scraping settings	--	--	--
		schedule:	A scraping schedule for the individual metric; overrides the the one specified in metricDefaults Setting example: If the schedule is set to every minute `0 * * ? * *`	Y	--	None

Item#				Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
	azureMetricConfiguration:			Azure metric configuration	--	--	--
		metricName:		The name of the metric in Azure Monitor to query For details on specifiable values, see *Metrics you can collect* in *3.15.1(1)(h) Promitor (Azure Monitor performance data collection capability)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.	Y	--	Varies depending on the metric.
		[limit:]		The maximum amount of resources to scrape when using dimensions or filters. If omitted, this is specified as the metricDefault.limit value.	Y	--	None
		[dimension:]		The dimension that should be used to scrape a multi-dimensional metric in Azure Monitor.	--	--	--
			name:	The name of the dimension that should be used to scrape a multi-dimensional metric in Azure Monitor.	Y	--	Varies depending on the metric.
		aggregation:		Aggregation settings	--	--	--
			type:	The aggregation that needs to be used when querying Azure Monitor	Y	--	Varies depending on the metric.
			[interval:]	Overrides the default aggregation interval defined in metricDefaults.aggregation.interval with a new interval	Y	--	None
	[resources:]			An array of one or more resources to get metrics for. The fields required vary depending on the resourceType being created, and are documented for each resource.	--	--	--
	-	<property>		The method of specification varies depending on the resourceType, such as the name of the resource. The following shows values to be specified: • If the resource type is VirtualMachine virtualMachineName • If the resource type is FunctionApp functionAppName, slotName (optional) • If the resource type is ContainerInstance containerGroup • If the resource type is KubernetesService clusterName • If the resource type is FileStorage accountName • If the resource type is BlobStorage accountName • If the resource type is ServiceBusNamespace namespace, queueName (optional), topicName (optional) • If the resource type is CosmosDb dbName	Y	--	Varies depending on the metric.

Item#			Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
			• If the resource type is SqlDatabase serverName, databaseName • If the resource type is SqlServer serverName • If the resource type is SqlManagedInstance instanceName • If the resource type is SqlElasticPool serverName, poolName • If the resource type is LogicApp workflowName			
		[resourceGroupName:]	Changes the resource group that contains resource. (Overrides azureMetadata.resourceGroupName)	Y	--	None
		[subscriptionId:]	Changes the subscription id to which the resource belongs. (Overrides azureMetadata.subscriptionId)	Y	--	None
	[resourceDiscoveryGroups:]		An array of one or more resource discovery groups that will be used to automatically discover all resources through Promitor Resource Discovery. For every found resource, it will get the metrics and report them.	--	--	--
	-	name:	Discovery group name.	Y	--	Varies depending on the metric.

Legend:

REQ: Required setting, Y: Modifiable, N: Not modifiable, --: Not applicable

#

Brackets ([]) denote optional items.

Promitor Scraper runtime configuration file (runtime.yaml)

Syntax

Written in YAML format.

```
authentication:
  mode: ServicePrincipal
  identityId:  client-ID
server:
  httpPort:  20719
metricSinks:
  prometheusScrapingEndpoint:
    enableMetricTimestamps:true
    baseUriPath: /metrics
metricsConfiguration:
  absolutePath:  installation-directory/jp1pccs/conf/promitor/scraper/metric
s-declaration.yaml
resourceDiscovery:
  host: installation-host-name
  enabled: true
  port: 20720
```

File

runtime.yaml

runtime.yaml.model (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\promitor\scraper\`

When using a logical host

shared-folder`\jp1ima\conf\promitor\scraper\`

For Linux

When using a physical host

`/opt/jp1ima/conf/promitor/scraper/`

When using a logical host

shared-directory`/jp1ima/conf/promitor/scraper/`

Description

The configuration file that defines Promitor Scraper authentication information, ports used for scraping, and other information.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in Promitor Scraper behavior when restarting Promitor Scraper.

After performing the action above, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

Item#	Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
authentication:	Authentication for Azure	--	--	--
[mode:]	Defines authentication mode to use. Options are ServicePrincipal, SystemAssignedManagedIdentity, If Promitor is on Azure, specifying SystemAssignedManagedIdentity or UserAssignedManagedIdentity is recommended. If Promitor is not on Azure, specify ServicePrincipal.	REQ	--	ServicePrincipal
[identityId:]	Id of the Azure AD entity to authenticate with when integrating with Microsoft Azure. Required when using ServicePrincipal.	REQ	--	None
[server:]	server settubgs	--	--	--
[httpPort:]	Defines the port to serve HTTP traffic If omitted, this is specified as 80.	Y	--	20719
[metricSinks:]	Metric Configuration	--	--	--
[prometheusScrapingEndpoint:]	Prometheus settings	--	--	--
[enableMetricTimestamps:]	Defines whether or not a timestamp should be included when the value was scraped on Azure Monitor. Supported values are True to opt-in & False to opt-out.	N	--	true
baseUriPath:	Controls the path where the scraping endpoint for Prometheus is being exposed.	N	--	`/metrics`
[metricsConfiguration:]	Metric Configuration	--	--	--
[absolutePath:]	Defines the location of the YAML file that declares what Azure Monitor metrics to scrape. Specify in a character string of 1 to 255 characters. If omitted, this is specified as `/config/metrics-declaration.yaml`.	Y	--	*installation-directory*`/jp1ima/conf/promitor/scraper/metrics-declaration.yaml`
[resourceDiscovery:]	Promitor Resource Discovery Agent settings	--	--	--

Item#		Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
	host:	DNS name of Promitor Resource Discovery agent.	Y	--	The host name is set when installing.
	[enabled:]	Indication whether or not resource discovery is enabled through the Promitor Resource Discovery agent. You can specify true or false.	Y	--	true
	port:	Port of Promitor Resource Discovery agent.	Y	--	20720

Legend:

REQ: Required setting, Y: Modifiable, N: Not modifiable, --: Not applicable

#

Brackets ([]) denote optional items.

Promitor Resource Discovery configuration file (resource-discovery-declaration.yaml)

Syntax

Written in YAML format.

```
verion: v1
azureLandscape:
  tenantId: tenant-ID
  subscriptions:
  - subscription-ID
resourceDiscoveryGroups:
  - name: virtual-machine-group
    type: VirtualMachine
  - name: function-app-group
    type: FunctionApp
```

File

resource-discovery-declaration.yaml

resource-discovery-declaration.yaml.model (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\promitor\resource-discovery\`

When using a logical host

shared-folder`\jp1ima\conf\promitor\resource-discovery\`

For Linux

When using a physical host

`/opt/jp1ima/conf/promitor/resource-discovery/`

When using a logical host

shared-directory`/jp1ima/conf/promitor/resource-discovery/`

Description

The configuration file that defines the resource group to be acquired by Promitor Resource Discovery.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in Promitor Resource Discovery behavior when restarting Promitor Resource Discovery.

After performing the action above, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

Item#					Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
version					Version of declaration that is used. Allowed values are v1.	N	--	v1
azureLandscape:					Azure information	--	--	--
	tenantId:				The id of the Azure tenant that will be queried.	REQ	Tenant ID	None
	subscriptions:				Defines a subset of subscriptions defined in the Azure landscape	--	--	--
	-	<subscriptionId>			List of Azure subscriptions in the Azure tenant to discover resources in.	REQ	Subscription ID	None
resourceDiscoveryGroups:					Defines a list of resource groups which contains the resources.	--	--	--
-	name:				Name of the resource discovery group which will be used in metrics declaration of Promitor Scraper. Specify this within 256 bytes.	Y	--	Varies depending on the resource discovery group.
	type:				Type of Azure resources that must be discovered, see "Supported Azure Services" for a full list of supported types. The following shows values that can be specified: • VirtualMachine • FunctionApp • ContainerInstance • KubernetesService • FileStorage • BlobStorage • ServiceBusNamespace • CosmosDb • SqlDatabase • SqlManagedInstane • SqlElasticPool • LogicApp	Y	--	Varies depending on the resource discovery group.
	[criteria:]				Conditions to be retrieved. Specify when you want to filter.	--	--	--
		include:			Specifies the conditions for acquisition targets.	--	--	None
			[subscriptions:]		A list of subscription(s) in which the resource is allowed to be located.	--	--	None
			-	<subscriptionId>	Specifies the subscription ID.	Y	--	None

Item#					Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
			[resourceGroups:]		A list of resource group(s) in which the resource is allowed to be located.	--	--	None
			-	<resourceGroupName>	Specifies the resource group name.	Y	--	None
			[tags:]		A list of Azure tags and the expected values (exact or regular expression) with which the resources have to be annotated.	--	--	None
				<key>:<value>	Specifies the Azure tag value. This can be specified using a regular expression.	Y	--	None
			[regions:]		A list of Azure region(s) in which the resource is allowed to be located.	--	--	None
			-	<region>	Species the region.	Y	--	None

Legend:

REQ: Required setting, Y: Modifiable, N: Not modifiable, --: Not applicable

#

Brackets ([]) denote optional items.

Promitor Resource Discovery runtime configuration file (runtime.yaml)

Syntax

Written in YAML format.

```
authentication:
  mode: ServicePrincipal
  identityId:  client-ID
server:
  httpPort:  20720
```

File

runtime.yaml

runtime.yaml.model (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\promitor\resource-discovery\`

When using a logical host

shared-folder`\jp1ima\conf\promitor\resource-discovery\`

For Linux

When using a physical host

`/opt/jp1ima/conf/promitor/resource-discovery/`

When using a logical host

shared-directory`/jp1ima/conf/promitor/resource-discovery/`

Description

The configuration file that defines Promitor Resource Discovery authentication information, ports used for scraping, and other information.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in Promitor Resource Discovery behavior when restarting Promitor Resource Discovery.

After performing the action above, definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed.

Content description

Item#		Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
authentication:		Authentication for Azure	--	--	--
	[mode:]	Defines authentication mode to use. Options are ServicePrincipal, SystemAssignedManagedIdentity, UserAssignedManagedIdentity. If Promitor is on Azure, specifying SystemAssignedManagedIdentity or UserAssignedManagedIdentity is recommended. If Promitor is not on Azure, specify ServicePrincipal.	REQ	--	ServicePrincipal
	[identityId:]	Id of the Azure AD entity to authenticate with when integrating with Microsoft Azure. Required when using ServicePrincipal.	REQ	--	None
[server:]		server settings	--	--	--
	[httpPort:]	Defines the port to serve HTTP traffic If omitted, this is specified as 80.	Y	--	20720

Legend:

REQ: Required setting, Y: Modifiable, --: Not applicable

#

Brackets ([ ]) denote optional items.

Script exporter configuration file (jpc_script_exporter.yml)

Syntax

Written in YAML format.

```
scripts:
  - name: run_scriptA
    command: ./examples/scriptA.sh
    timeout:
      max_timeout: 120
  - name: run_scriptB
    command: ./examples/scriptB.sh
    args:
      - arg1
      - arg2
```

File

`jpc_script_exporter.yml`

`jpc_script_exporter.yml.model` (Model file)

Storage directory

For Windows

When using a physical host

Agent-path`\conf\`

When using a logical host

shared-folder`\jp1ima\conf\`

For Linux

When using a physical host

`/opt/jp1ima/conf/`

When using a logical host

shared-directory`/jp1ima/conf/`

Description

The configuration file that determines the behavior of Script exporter.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

When Script exporter is restarted.

Content description

Item#			Description	Modifiable	Content set by the user in JP1/IM - Agent	Default value in JP1/IM - Agent
scripts:			Script settings	--	--	None
-	name:		The name of the script. It must be a valid Prometheus label value (Unicode characters). Specify in a character string within 1 to 255 characters.	REQ	Name of the script being monitored (any name)	None

	command:		Specify the script to be executed. For the output format of the script, see the description of Prometheus Text-based format in *3.15.1 Performance monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
			Setting example:
			`"/bin/foo"`
			Example of output:
			`# HELP metric_name description`
			`# TYPE metric_name gauge`
			`metric_name {label1="labelvalue1"} 12345`
			`metric_name {label1="labelvalue2"} 67890`
				REQ	Script being monitored	None

	args:		All arguments.
			Setting example:
			`- "--output"`
			`- "/dev/null"`
				REQ	Script arguments (not required if no arguments are used)	None

	timeout:		Timeout settings	Y	--	None
		max_timeout:	It limits the maximum timeout value that requests can specify; a request that specifies a larger timeout will have the timeout adjusted down to the max_timeout value. Specify this value in seconds. If omitted, this is specified as the timeout value set in Prometheus.	Y	Number of seconds until timeout	None
		enforced:	If enforced is true, script_exporter attempts to enforce the timeout by killing the script's main process after the timeout expires. The default is to not enforce timeouts. You can specify true or false. If omitted, this is specified as false.	Y	Whether to forcibly terminate the script when timed out	None

Legend:

REQ: Required setting, Y: Modifiable, --: Not applicable

#

Brackets (`[]`) denote optional items.

Sample file of Script exporter configuration file for SAP system monitoring (jpc_script_exporter_sap.yml)

Format

This example is provided as sample to monitor SAP in the following conditions.

- Conditions

<Common the SAP system log extract commands>

- The prerequisites described in *3.15.5 SAP system monitoring function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide* are met.
- The path relative to the working folder specified in the Script exporter service definition file, and the environment parameters file is stored in the following folder.

  ```
  ../conf/user/
  ```

- IM management node categories

  Enterprise
- Specify a max_timeout value that is less than the Prometheus server scrape interval. Since the value of the max_timeout is set to 30, change the value of max_timeout if the Prometheus server scrape interval is less than or equal to 30.

<jr3slget command>

- Output system log information of SAP instance "o246bci_SD5_00".
- The following information was specified in the environmental parameters file (jr3slget.ini) when the command was executed to extract system log information:
  - RFC access information
  - Target information
  - Log file to which the system log information is output
  - Command working directory
- The timestamp file is stored in the jr3slget folder below the working folder specified in the environment parameters file.
- Label name of IM management node: SAP Syslog extractor(jr3slget)

<jr3alget command>

- Specify "SAP CCMS Monitor Templates" for the monitor set name and "Entire System" for the monitor name to print CCMS alert message.
- The following information is specified in the environment parameters file (jr3alget.ini) when extracting CCMS alert information by executing the command.
  - RFC access information
  - Target information
  - Log file to which CCMS alerting information is output
  - Command working directory

- The timestamp file is stored in the jr3slget folder below the working folder specified in the environment parameters file.
- Label name of IM management node: SAP CCMS Alert extractor(jr3alget)

- Definition example

```
scripts:
  - name: SAP Syslog extractor(jr3slget)
    command: jr3slget-command-path
    args:
      - "-lasttime"
      - "sltimestamp.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3slget.ini"
    timeout:
      max_timeout: 30
      enforced: true

  - name: SAP CCMS Alert extractor(jr3alget)
    command: jr3alget-command-path
    args:
      - "-lasttime"
      - "altimestamp.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3alget.ini"
    timeout:
      max_timeout: 30
      enforced: true
```

File

`jpc_script_exporter_sap.yml`

Storage directory

- Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\sample\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/sample/`

Description

This configuration file defines Script exporter operation for SAP system monitoring. Copy the sample file (jpc_script_exporter_sap.yml), change the file name of the destination to "jpc_script_exporter.yml", and place it in the placement destination of the Script exporter configuration file (jpc_script_exporter.yml). For the location of the files, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Character code

See to the explanation of *Character encoding* in *Script exporter configuration file (jpc_script_exporter.yml)*.

Line feed code

See the explanation of *Line feed code* in *Script exporter configuration file (jpc_script_exporter.yml)*.

When the definitions are applied

See the explanation of *When the definitions are applied* in *Script exporter configuration file (jpc_script_exporter.yml)*.

Information that is specified

See the explanation of *Information that is specified* in *Script exporter configuration file (jpc_script_exporter.yml)*.

When you define a script in Script exporter configuration file that executes the SAP system log extract command, script.name must include the SAP system log extract command name (jr3slget, or jr3alget) to be executed. Otherwise, an IM management node for the metric output function of SAP system monitoring is created under Other Applications category.

When you create multiple environment parameters file that differ in parameter settings, such as when defining multiple RFC destinations (multiple instance), you define multiple scripts as shown in the following example definition.

```
scripts:
  - name: SAP Syslog extractor(jr3slget)_A
    command: C:/Program Files (x86)/Hitachi/jp1pc/agtm/evtrap/jr3slget.exe
    args:
      - "-lasttime"
      - "sltimestamp_A.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3slget_A.ini"
    timeout:
      max_timeout: 30
      enforced: true

  - name: SAP CCMS Alert extractor(jr3alget)_A
    command: C:/Program Files (x86)/Hitachi/jp1pc/agtm/evtrap/jr3alget.exe
    args:
      - "-lasttime"
      - "altimestamp_A.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3alget_A.ini"
    timeout:
      max_timeout: 30
      enforced: true

  - name:  SAP Syslog extractor(jr3slget)_B
    command: C:/Program Files (x86)/Hitachi/jp1pc/agtm/evtrap/jr3slget.exe
    args:
      - "-lasttime"
      - "../data/script_exporter/jr3slget/sltimestamp_B.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3slget_B.ini"
    timeout:
      max_timeout: 30
      enforced: true

  - name:  SAP CCMS Alert extractor(jr3alget)_B
    command: C:/Program Files (x86)/Hitachi/jp1pc/agtm/evtrap/jr3alget.exe
    args:
      - "-lasttime"
      - "altimestamp_B.txt"
      - "-x2"
      - "-cnf"
      - "../conf/user/jr3alget_B.ini"
    timeout:
      max_timeout: 30
      enforced: true
```

Log monitoring common definition file (jpc_fluentd_common.conf)

Format

```
@include jpc_fluentd_common_wevt_rendered.conf (Windows only)
@include jpc_fluentd_common_list.conf

## [System Settings]
<system>
  log_level log-level
  format text
  time_format %Y-%m-%d %H:%M:%S %z
  workers number-of-workers
</system>

<worker 0>
## [Remote Write Settings]
  <filter jpc_ima_metrics.**>
    @type record_transformer
    enable_ruby true
    auto_typecast true
    renew_record true

    <record>
      labels ${record}
      samples ${[[time.utc.to_i*1000,1]]}
    </record>
  </filter>

  <match jpc_ima_metrics.**>
    @type http
    headers {"accept":"application/json"}
    content_type application/json
    json_array false
    endpoint Trend data writing API of the integrated agent control base
    <buffer>
      flush_interval 60s
      disable_chunk_backup true
    </buffer>
  </match>
</worker>

<worker 1-worker id>
## [Output Settings]
  <match {tail.*.jp1event,winevt.*.jp1event}>
    @type copy
    copy_mode no_copy
    <store>
      @type http
      endpoint JP1 Event Conversion API of Unified Agent Control Platform
      headers {"accept":"application/json"}
      content_type application/json
      json_array true
      open_timeout 60
      read_timeout 60
      error_response_as_unrecoverable true
      retryable_response_codes [503]
      <buffer tag>
        @type file
        flush_interval flush-interval
        overflow_action Output plug-in behavior when the buffer queue is fu
ll
        retry_wait Retry interval
        path ../data/fluentd/buffer
        timekey_wait 600
        timekey_use_utc false
        timekey_zone local timezone
        chunk_limit_size 32MB
        total_limit_size Buffer size limit
        chunk_full_threshold 0.95
        queued_chunks_limit_size 1
        compress text
        flush_at_shutdown false
        flush_mode default
        flush_thread_count 1
        flush_thread_interval 1.0
        flush_thread_burst_interval 1.0
        delayed_commit_timeout 60
        retry_forever true
        retry_type periodic
        retry_wait 10s
        disable_chunk_backup false
      </buffer>
    </store>
    <store>
      @type relabel
      @label @STDOUT
    </store>
  </match>

## [Private Settings]
  <match {tail.*.outputlog,wevt.*.outputlog}>
    @type relabel
    @label @STDOUT
  </match>

  <label @STDOUT>
    <match {tail.**,wevt.**}>
      @type stdout
      <format>
        @type out_file
        time_type string
        time_format %Y-%m-%d %H:%M:%S %z
        localtime true
        utc false
      </format>
    </match>
  </label>
</worker>
```

File

`jpc_fluentd_common.conf`

`jpc_fluentd_common.conf.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

A File for defining Common behavior in log monitoring function, such as HTTP POST request function and log output function.

Lines that begin with a "#" are treated as Comment and do not affect programming behavior.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This information is reflected in Fluentd operation when Fluentd serviceis Restart.

Information that is specified

`<worker> Directive`

By specifying the ID of the worker that Fluentd starts as an argument, the plug-in specified in the directive will be operated only on the worker with the specified ID.

worker id (Option)

Specifies the ID of the worker that Fluentd will start. Serves as an argument to the worker N-M directive. N always specifies 1. The value specified for M specifies the integer specified for the number of workers minus one.

`[System Settings] Section`

Performs a Setup that affects the operation of the entire log monitoring function.

Log Level (Optional)

Specifies the log level for Fluentd.

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
The following log levels can be specified in ascending order of redundancy: • fatal • error • warn • info • debug • trace Default is "info". Fluentd outputs info,warn,error, and fatal logs in default.	Can be changed	Setup it according to the logs you want to check.	info

number-of-workers (Optional)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Specifies the number of workers that Fluentd will start. Valid values are integers from 1 to 31.	Can be changed	Specify the total number of log monitoring common definition files, text log file monitoring definition files, Windows event log monitoring definition files, and log metrics definition files.	10

`[Output Settings] Section`

Executes setup for outputting the log data monitored by log monitoring function.

JP1/IM agent control base's JP1 event-translation API (optional)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value

Specifies the endpoint for HTTP request, up to 512 bytes. If you use HTTPS, use https prefix.
<Sample Setup>
`# Use HTTP`
`endpoint http://example.com/api`
`# Use HTTPS. You can set additional HTTPS parameters like tls_xxx`
`endpoint https://example.com/api`
This parameter supports placeholders, so you can embed time, tags, and record fields. The <buffer> section is also required for the placeholders to work.
<Sample Setup>
`endpoint http://example.com/api/${tag}-${key}`
`<buffer tag,key>`
`# buffer parameters`
`</buffer>`
Specifies the destination of the log data and metric in endpoint. For details, see *(9) HTTP POST request function (http plug-in)* of *3.15.3 Log monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
If URL specified in endpoint is incorrect, Warning Message is issued and no metric or log data is sent. Therefore, after Fluentd
	Setup Required	Specifies JP1 event translation API's URL for JP1/IM agent control base to issue JP1 events. If you have changed the Port number of JP1/IM agent control base, you must change Setup.	`http://`*integrated-agent-host-name*`:20726/ima/api/v1/proxy/service/imdd/im/api_system/v1/events/transform`

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
starts, you must ensure that no Warnings appear in the log at POST of metric and log data.			

Flush interval (option)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Specify how often to send log data stored in buffer to JP1/IM agent control base. Value that you can specify is 1s to 86,400s. The unit (s) is required. It also works without a specification.	Yes	Change the sending intervals.	60s

How output Plug-In Works When the Buffer Queue Is Full (Optional)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Determines how output plug-in behaves when buffer queue is full. The following Values can be specified: • throw_exception Prints Error to Fluentd logs. Even if a new log is output to the log File to be monitored, it is not added to the buffers. When the transmission is successful, the log output to the log File is trapped, but if it is wrapped and deleted, it is lost. • drop_oldest_chunk Delete the oldest chunk to accept the new chunk.	Yes	Determines how output plug-in behaves when buffer queue is full.	throw_exception

Retry interval (option)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Specifies the retry interval for chunks that have failed to be sent. Value that you can specify is 1s to 600s. The unit (s) is required. If Value is specified for this parameter in a blank or invalid format, the retry interval is about 2 seconds in Winsows environment and about 0.02 seconds in Linux environment.	Yes	Specify the retry interval.	10s

Buffer size limit (option)

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Specifies the size limit for the instance of the buffer plugin. Possible values are 32MB~65536MB. If the total size of the buffers stored reaches this threshold, all add operations fail with an error and data is lost. The buffer uses the amount of disk space in the environment where JP1/IM - Agent is set up. The total size of the buffer is estimated by the following formula. "0.015MB * Number of JP1 events to buffer"	Yes	Specifies the size limit for the instance of the buffer plugin.	4096MB

`[Remote Write Settings] Section`

Fluentd performs a Setup to send sample to Trend data Management Database of JP1/IM - Manager.

JP1/IM agent control base Trend Data Write API (Optional)

Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value

Specifies the endpoint for HTTP request, up to 512 bytes. If you use HTTPS, use https prefix.
<Sample Setup>
`# Use HTTP`
`endpoint http://example.com/api`
`# Use HTTPS. You can set additional HTTPS parameters like tls_xxx`
`endpoint https://example.com/api`
This parameter supports placeholders, so you can embed time, tag, and record fields. The <buffer> section is also required for the placeholders to work.
<Sample Setup>
`endpoint http://example.com/api/${tag}-${key}`
`<buffer tag,key>`
`# buffer parameters`
`</buffer>`
Specifies the destination of the log data and metric in endpoint. For details, see *(9) HTTP POST request function (http plug-in)* of *3.15.3 Log monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
If URL specified in endpoint is incorrect, Warning Message is issued and no metric or log data is sent. Therefore, after Fluentd starts, you must ensure that no Warnings appear in the log at POST of metric and log data.
	Setup Required	Specifies URL of the trend data write API for JP1/IM agent control base to send metric to JP1/IM - Manager. If you have changed Port number of JP1/IM agent control base, you must change Setup.	`http://`*integrated-agent-host-name*`:20727/ima/api/v1/proxy/service/promscale/write`

`[Private Settings] Section`

Cannot be edited.

Example definition

```
## [System Settings]
<system>
  log_level info
  format text
  time_format %Y-%m-%d %H:%M:%S %z
  workers 10
</system>

<worker 0>
## [Remote Write Settings]
  <filter jpc_ima_metrics.**>
    @type record_transformer
    enable_ruby true
    auto_typecast true
    renew_record true

    <record>
      labels ${record}
      samples ${[[time.utc.to_i*1000,1]]}
    </record>
  </filter>
  <match jpc_ima_metrics.**>
    @type http
    headers {"accept":"application/json"}
    content_type application/json
    json_array false
    endpoint http://integrated-agent-host-name:20727/ima/api/v1/proxy/servic
e/promscale/write
    <buffer>
      flush_interval 60s
      disable_chunk_backup true
    </buffer>
  </match>
</worker>

<worker 1-9>
  ## [Output Settings]
  <match {tail.*.jp1event,wevt.*.jp1event}>
    @type copy
    copy_mode no_copy
    <store>
      @type http
      endpoint http://integrated-agent-host-name:20726/ima/api/v1/proxy/serv
ice/imdd/im/api_system/v1/events/transform
      headers {"accept":"application/json"}
      content_type application/json
      json_array true
      open_timeout 60
      read_timeout 60
      error_response_as_unrecoverable true
      retryable_response_codes [503]
      <buffer tag>
        @type file
        flush_interval 5s
        overflow_action throw_exception
        retry_wait 10s
        path ../data/fluentd/buffer
        timekey_wait 600
        timekey_use_utc false
        timekey_zone local timezone
        chunk_limit_size 32MB
        total_limit_size 4096MB
        chunk_full_threshold 0.95
        queued_chunks_limit_size 1
        compress text
        flush_at_shutdown false
        flush_mode default
        flush_thread_count 1
        flush_thread_interval 1.0
        flush_thread_burst_interval 1.0
        delayed_commit_timeout 60
        retry_forever true
        retry_type periodic
        retry_wait 10s
        disable_chunk_backup false
      </buffer>
    </store>
    <store>
      @type relabel
      @label @STDOUT
    </store>
  </match>

## [Private Settings]
  <match {tail.*.outputlog,wevt.*.outputlog}>
    @type relabel
    @label @STDOUT
  </match>

  <label @STDOUT>
    <match {tail.**,wevt.**}>
      @type stdout
      <format>
        @type out_file
        time_type string
        time_format %Y-%m-%d %H:%M:%S %z
        localtime true
        utc false
      </format>
    </match>
  </label>
</worker>
```

Log monitoring target definition file (jpc_fluentd_common_list.conf)

Format

```
## [Target Settings]
@include monitor-definition-file-name
...
```

File

`jpc_fluentd_common_list.conf`

`jpc_fluentd_common_list.conf.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

A File that specifies what to monitor for logging. Specifies File of text-formatted monitoring log file definition file, or monitoring Windows event-log definition file. The monitoring loggging of the specified monitoring definition File is set to Enable.

In the default Setup, the logging monitoring for all "monitoring text-formatted log file definition file" and "monitoring Windows event-log definition file" under conf/user directory is Enable, as defined below.

- Default Setup

```
## [Target Settings]
@include user/fluentd_*_tail.conf
@include user/fluentd_*_wevt.conf (Windows only)
```

Lines that begin with a "#" are treated as Comment and do not affect programming behavior. If you want to perform an operation that temporarily stops log monitoring for some monitor definition File, enumerate the monitor definition File and Comment out the monitor definition File row that you want to stop log monitoring.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This information is reflected in Fluentd operation when Fluentd serviceis restart.

Information that is specified

`[Target Settings] Section`

Setup the monitor-definition File that you use in fluentd.

Monitor Definition File Name (Optional)

By specifying File of definition file for monitoring text-formatted log file or definition file for monitoring Windows event-log, the logging monitoring of the specified monitor-definition File is set to Enable. The asterisk (*) in the monitor-definition File represents a wildcard (arbitrary character string). The only wildcard you can specify is "*".

If this option is omitted, log monitoring is not performed.

It is not case sensitive in Windows. It is case sensitive in Linux.

You can specify the monitor definition file up to 1016 in Windows and up to 508 in Linux.

Example definition

In the following example, the fluentd_abcd_tail.conf and fluentd_abcd_wevt.conf monitoring definitions File have Setup of Enable, and Setup of the fluentd_efgh_tail monitoring definition File is disabled.

```
## [Target Settings]
@include fluentd_abcd_tail.conf
#@include fluentd_efgh_tail.conf
@include fluentd_abcd_wevt.conf
```

Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)

Format

```
<worker 0>
## [Metric Settings]
<source>
  @type exec
  command "echo {}"
  <parse>
    @type json
  </parse>
  run_interval 60s
  tag jpc_ima_metrics.tail.log-monitoring-name
</source>

<filter jpc_ima_metrics.tail.log-monitoring-name>
  @type record_transformer
  enable_ruby true
  auto_typecast false
  <record>
    __name__ fluentd_logtrap_running
    instance host-name
    jp1_pc_nodelabel IM-management-node-label-name
    jp1_pc_category category-ID
    jp1_pc_logtrap_defname log-monitoring-name_tail
    jp1_pc_trendname fluentd
    job jpc_fluentd
    jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
    jp1_pc_addon_program JPC Fluentd
  </record>
</filter>
</worker>
<worker worker id>
## [Input Settings]
<source>
  @type tail
  tag tail.log-monitoring-name
  path monitored-paths
  follow_inodes true
  refresh_interval 60
  skip_refresh_on_startup false
  read_from_head read-the-logs-to-be-monitored-when-Fluentd-is-started-for-the-first-time-from-the-beginning
#  encoding "Fluentd-character-code"
#  from_encoding "character-codes-of-monitored-logs"
  read_lines_limit 1000
  read_bytes_limit_per_second -1
  pos_file ../data/fluentd/tail/log-monitoring-name.pos
  path_key tailed_path
  rotate_wait 5s
  enable_watch_timer enable-additional-watch-timers
  flush-interval-for-multiline-logs
  enable_stat_watcher true
  open_on_every_update false
  emit_unmatched_lines false
  ignore_repeated_permission_error false
  <parse>
    @type log-format
    settings-depending-on-the-log-format
  </parse>
</source>

## [Attributes Settings]
<filter tail.log-monitoring-name>
  @type record_transformer
  enable_ruby true
  auto_typecast false
  renew_record true

  <record>
    ID event-ID
    MESSAGE ${record["message"]}
    JP1_SOURCEHOST host-ame
    JPC_LOG_TIME ${time.utc.to_i}
    PRODUCT_NAME /HITACHI/JP1/JPCCS2/LOGTRAP/IM-management-node-label-name
    PPNAME /HITACHI/JP1/JPCCS2
    SEVERITY severity
    PLATFORM ${ if RUBY_PLATFORM.downcase =~ /mswin(?!ce)|mingw|cygwin|bccwi
n/; 'NT'; else 'UNIX'; end }
    OBJECT_TYPE LOGFILE
    OBJECT_NAME ${record['tailed_path']}
    ROOT_OBJECT_TYPE LOGFILE
    ROOT_OBJECT_NAME ${record['tailed_path']}
    JP1_TRAP_NAME ${tag_parts[1]}
    JPC_NODELABEL IM-management-node-label-name
    any-attribute-name any-value
  </record>
</filter>

## [Inclusion Settings]
#<filter tail.log-monitoring-name>
#  @type grep
#  <regexp>
#    key attribute-name-of-JP1-event
#    pattern /regular-expression-of-logs-to-monitor/
#  </regexp>
#</filter>

## [Exclusion Settings]
#<filter tail.log-monitoring-name>
#  @type grep
#  <exclude>
#    key attribute-name-of-JP1-event
#    pattern /regular-expressions-for-logs-that-you-do-not-want-to-monitor/
#  </exclude>
#</filter>

## [Forward Settings]
<match tail.log-monitoring-name>
  @type rewrite_tag_filter
  <rule>
    key attribute-name-of-JP1-event
    pattern /regular-expression-for-logs-that-emit-JP1-events/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key SEVERITY
    pattern /.*/
    tag ${tag}.outputlog
  </rule>
</match>

<filter /tail\.log-monitoring-name\.(jp1event|outputlog)/>
  @type record_transformer
  enable_ruby true
  auto_typecast true
  renew_record true
  <record>
    eventId ${record['ID']}
    xsystem true
    message ${record['MESSAGE']}
    attrs ${record}
  </record>
  remove_keys $.attrs.ID
  remove_keys $.attrs.MESSAGE
</filter>
</worker>
```

File

`fluentd_@@trapname@@_tail.conf.template`

`fluentd_@@trapname@@_tail.conf.template.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

Definition File for monitoring text-formatted logging File.

Copy the template (`fluentd_@@trapname@@_tail.conf.template`) and change file name of Copy destination to `fluentd_`*log-monitoring-name*`_tail.conf` for use. File name must be unique within integrated agent host. For details on the location of `fluentd_`*log-monitoring-name*`_tail.conf`, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. *log-monitoring-name* must be between 1 and 30 characters long. Allowed characters are single-byte alphanumeric characters, "`-`" (hyphen), and "`_`" (underscore).

Create a monitor-definition file for each wrapped-around log file group that you want to monitor (or for each log file that does not wrap-around). JP1/IM - Agent creates a IM managed node for SID of target of monitoring according to the value specified in *IM-management-node-label-name* of the IM managed node in the monitoring definition file. If another monitoring definition file has the same *IM-management-node-label-name*, only one IM management node is created.

The text-based log file monitoring feature reads this definition file and analyzes the log that the application has written to the text-based log file. You can setup if you specify a condition for the analyzed information and the condition is met, the information to be converted to JP1 events or output to Fluentd logging file. For details about JP1 event to be issued, see *3.2.3(2) JP1 event issued that monitoring a textual log File*.

Lines beginning with "`#`" are treated as Comment and do not affect the programming behavior.

The default definition in `[Forward Settings]` section is set to transform log data to JP1 event and transfer to JP1/IM - Manager when `SEVERITY` is worse than `Warning`.

When transforming log data to JP1 event and transferring it to JP1/IM - Manager, set `SEVERITY` so that its severity is equal or worse than `Warning`.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This information is reflected in Fluentd operation when Fluentd service is restart.

If add or delete of definition files or value in `[Metric Settings]` section is changed, the change is reflected in tree view of the Integrated Operation Viewer window.

For details about application method, see *1.21.2(16) Creation and import of IM management node tree data (for Windows) (mandatory)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Information that is specified

`<worker>` directive

See the description of *<worker> directive* in *Log monitoring common definition file (jpc_fluentd_common.conf)*.

worker-id (optional)

Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Specifies the number of workers that Fluentd will start. Serves as an argument to the `<worker` *N*`>` directive. Valid values are integers from 1 to 128.	Can be changed	It must be specified so as not to duplicate the worker ID specified in the existing text log file	1

Description	Changea bility	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
		monitoring definition file or the Windows event log monitoring definition file.	

`[Metric Settings]` section

Setup Value of label of sample that you want to send to JP1/IM - Manager's Trend data Management Database.

log-monitoring-name (mandatory)

Specifies *log-monitoring-name* specified in the file name of copy destination as a string of 1 to 30 characters. Allowed characters are single-byte alphanumeric characters, "`-`" (hyphen), and "`_`" (underscore). The default value is "`@@trapname@@`".

Because you need to setup several locations in the file, use OS command/editor function to replace the "`@@trapname@@`" location with *log-monitoring-name* you want to specify.

If the specification is omitted, error occurs when Fluentd is started.

Note that *log-monitoring-name* must be setup as follows:

- All *log-monitoring-name* in the same file are the same.
- *log-monitoring-name* is unique for the monitoring text-formatted log file definition file and the Windows event log monitoring definition file

host-name (optional)

Specify the host name to be monitored using characters 1 to 255 other than control characters. The default value is setup by integrated agent installers.

If the specification is omitted, IM management node is not created.

You can also dynamically setup the canonical host name of the system by doing the following:

```
    instance ${Socket.gethostname}
```

IM-management-node-label-name (optional)

Specifies the character string that integrated operation viewer displays on IM management node label. This is not a control character. When URL is encoded, the character string must be between 1 and 234 bytes (the upper limit for multibyte characters is 26). The default value is "Application".

If the specified information is invalid or omitted, IM management node is not going to be created.

You can specify the same IM management node label name in different monitoring definition files. Then, only one IM management node is created, and JP1 events in both of monitor-defined files are Add to one IM management node.

category-ID (optional)

Specifies the category ID of IM management node corresponding to SID to be monitored for logging as a character 1 to 255 other than control characters. If the specification is omitted, "`otherApplications`" is assumed.

`[Input Settings]` section

Setup the path to the text-formatted log File that you want to monitor and the regular expressions that parse the log Message.

log-monitoring-name (mandatory)

Same as the section [Metric Settings] description.

monitored-paths (required)

Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
Specify the path to read. You can specify multiple paths by separated by commas. You can include `*` and strftime formats to dynamically add and delete the logging file you want to monitor. The list of log files is updated at `refresh_interval` intervals. For specification examples, see *(3) Text-format log file monitoring facility (tail plug-in)* in *3.15.3 Log monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. If you specify an incorrect path, Log Files logging is not read. The following rules apply to programming: • Specify as an absolute path • Directories and File on network drives cannot be specified (for Windows) • Specify "`/`" instead of "`\`" as the path delimiter (in Windows) • Multiple paths can be specified. • You can specify "`*`" (wildcard). • You specify within 256 bytes. • The following path names cannot be specified. - File with a leading "`-`" (hyphen) - Folder name, directory name, or File name containing environment-dependent characters - Space-directory-name (for Linux)	Installation Required	Specifies Log Files path.	Not applicable

read-the-logs-to-be-monitored-when-Fluentd-is-started-for-the-first-time-from-the-beginning (optional)

Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
Specifies whether the log should start reading from the beginning, not the end, or from the last read position recorded in `pos_file`. You can specify `true` or `false`.	Can be changed	If you want to read a log that was already Add at startup, change it to `true`.	false

Fluentd-character-code (optional)

If *character-codes-of-monitored-logs* is UTF-8 or C (handled as Comment), specify the default setup (handled as Comment). Specify UTF-8 if *character-codes-of-monitored-logs* is not UTF-8 nor C (handled as Comment). In the default Setup, since "`#`" is specified at the beginning of the line and it is handled as Comment, "`#`" is turned Delete.

Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent

Specifies the encoding in which to read the line.
By JP1/IM - Agent, in_tail outputs value of string in ASCII-8BIT encoding in default.
You can change it with the following options:
• `encoding` changes the text to `encoding`.
• If both `encoding` and `from_encoding` are specified, in_tail attempts to convert the *`jj`*`,` string to a `encoding`.
	Can be changed	In JP1/IM - Agent, you can specify the following Value:
		• `UTF-8`
			Not specified (Comment out)
			`#`
			`encoding "UTF-8"`

character-codes-of-monitored-logs (optional)

If *character-codes-of-monitored-logs* is UTF-8 or C, specify the default setup (handled as comment). If *character-codes-of-monitored-logs* is not UTF-8 nor C, specify the character code. In the default setup, since "#" is specified at the beginning of the line and it is handled as comment, "#" is turned delete.

Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
See the explanation of *Fluentd-character-code* (optional).	Can be changed	Specifies the character encoding of log files. In JP1/IM - Agent, you can specify the following value: • `UTF-16LE` • `UTF-16BE` • `Shift_JIS` • `Windows-31J` • `GB18030`	Not specified (Comment out) `# encoding "Shift_JIS"`

enable-additional-watch-timers

Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
Specify `true` or `false`. If `false` is specified for this parameter, the most recent log is not monitored when reading multiple lines of log. Therefore, if multiline is specified as the `type` of the parse plug-in, `true` is specified. Specifying `false` for this parameter significantly reduces CPU and I/O consumption when tailing a large number of files on systems that support inotify.	Can be changed	Specify `true` only if `multiline` is specified as the `type` of the parse plugin.	false

flush-interval-for-multiline-logs

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
multiline_flush_interval	Specify `multiline_flush_interval` item as flush interval for multiline logs. If this item is not specified, the latest log is not monitored when multiline logs are monitored. Therefore, when `type` of parsing plugin is set `multiline`, set it as following: `multiline_flush_interval 5s`	Changeable	Set `5s` only when `type` of parsing plugin is `multiline`.	`5s`

log-format

Specifies the format for parsing the imported log.

The following formats can be specified:

type	Description
none (Default)	Read a one-line log as it is without parsing or structuring.
regexp	Reads a single-line log that matches the pattern specified by the regular expression.
multiline	Loads a multi-line log that matches the pattern specified by the regular expression.
syslog	Read the log output by syslog.

type	Description
csv	Load logs in CSV format (comma delimited).
tsv	Loads logs in TSV format (tab-delimited).
ltsv	Import logs in LTSV format (labeled tab-delimited).

For examples of specifying logs in each format, see *3.15.3(3)(g) Log parsing function (parse plug-in)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

settings-depending-on-the-log-format

Specify the entries according to the *log-format*.

- If none

```
<parse>
  @type none
  message_key message
  time_key time
  null_empty_string false
  estimate_current_event true
  keep_time_key false
</parse>
```

- If regexp

```
<parse>
  @type regexp
  expression regular-expressions-to-parse-logs
  time_key time
  null_empty_string false
  estimate_current_event true
  keep_time_key false
  items-for-parsing-date-and-time-of-logs
</parse>
```

regular-expression-to-parse-log (required)

When using the Named Capture fieature to trim character strings, one of names is necessary to be "message". If character strings named "message" is not trimmed, MESSAGE of JP1 event will be empty.

Specifies a regular expression and parses the contents of one line of the log. Use the Named Capture feature to trim a string named "message" that Setup to Message of JP1 event. For example: The default Value contains a regular expression that trims the entire line in "message". You can also trim with another name and Setup to any property of JP1 event.

items-for-parsing-date-and-time-of-logs

When a Date/time in the logging Message is trimmed as the name "time", it is set as value of JPC_LOG_TIME of JP1 event. When you trim a Date/time in the logging Message as the name "time", it is necessery to define the items for parsing date and time of logs. When you do not trim a Date/time, or define the items for parsing date and time of logs are not defined, the value of JPC_LOG_TIME will be Date/time when Fluentd monitored the log message.

Item Name	Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
expression	specifies the regular expressions matches for logging. Regular expressions must be sandwiched between "/"	Can be changed	Setup according to Log Files logging format.	expression /^(?<message>.*)$/

Item Name	Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
	(delimiters). If the delimiter is not used, an error is output. Regular expressions must specify at least one named capture (?<*name*>*Regular expression for truncated logs*). Regular expressions can have i and m suffixes. - i(ignorecase) Ignores the case of the match. - m (multi-line) Creates a regular expression as a multi-line mode. ". " matches to a line break. - both Specify both i and m. If the log read does not Match the regular expression, the following Warning Message is printed in Fluentd log and the log is not going to be monitored. `2022-01-23 12:34:56 +0900 [warn]: #0 pattern not matched: "Error Message"`			
time_type	Specify type of the date and time of log to be parsed.	Changeable	Specify type of time according to the format of the log file to be monitored. Available time zone format: - unixtime Seconds from Epoch (e.g. 1510544815) - string Use format specified by time_format	--
time_format	Specify the time format within 256 bytes. Used to trim logs with the name "time". Processes values according to the specified format. It is available if the time_type is string. The following formats are supported: - `%b` Abbreviated month (Jan,Feb,...) - `%d` Day (01~31) - `%H` 24-hour clock (00~23) - `%M` min (00~59) - `%m` Month number (01~12) - `%S` sec (00~60 (60 indicatesleap second))	Changeable	Specify the time format according to the format of the log file to be monitored.	--

Item Name	Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent

	• `%Y`
	A number representing the year
	• `%N`
	fractional seconds
	If you specify an incorrect value, a warning message similar to the one shown below may be output to the Fluentd log, and the log may not be monitored.
	`2022-09-08 17:15:10 +0`
	`900 [warn]: #0 invali`
	`d line found file="C:/`
	`fluentd/install/log/ap`
	`p1/20220906_log1_utf8.`
	`txt"`
	`line="2022/12/3 12:34:`
	`56 jpcagt0 00004864 0`
	`0008904 agent.cpp 572`
	`KAVL99999-E \xE3\x82\x`
	`A8\xE3\x83\xA9\xE3\x83`
	`\xBC\xE3\x83\xA1\xE3\x`
	`83\x83\xE3\x82\xBB\xE3`
	`\x83\xBC\xE3\x82\xB8(2`
	`022/09/0817:15:09.24)`
	`" error="invalid timef`
	`ormat: value = 2022/12`
	`/3 12:34:56, error_cla`
	`ss = ArgumentError, er`
	`ror =string doesn't ma`
	`tch"`
	If this parameter is omitted, the time set to JPC_LOG_TIME is the time when Fluentd detected the log message. If syslog is specified for type and this parameter is not specified, no error or warning message is printed and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.			

localtime	Specify true because local time is used.	Not changeable	`true`	`true`
utc	Specify false because local time is used.	Not changeable	`false`	`false`
timezone	Date/time is parsed in specified `timezone`.	Changeable	Specify the timezone according to the format of the log file to be monitored. Available time zone format: • `[+-]HH:MM` e.g. `"+09:00"` • `[+-]HHMM` e.g. `"+0900"`	--

Item Name	Description	Changeability	What You Setup in Your JP1/IM - Agent	Default Value for JP1/IM - Agent
			When `timezone` is specified, `time_format` is must be specified.	

(Legend) -: Not applicable

- For multiline

```
<parse>
  @type multiline
  format_firstline regular-expression-to-parse-the-first-line-log
  formatN regular-expression-to-parse-logs
  time_key time
  null_empty_string false
  estimate_current_event true
  keep_time_key false
  items-for-parsing-date-and-time-of-logs
</parse>
```

regular-expression-to-parse-the-first-line-log (required)

Specify a regular expression to parse the contents of one log line. If the specified regular expression matches the contents of the log, the matched log line is read as the first line of a multi-line log.

regular-expression-to-parse-logs (required)

Similar to the description in "For regexp". N can be an integer from 1 to 20, and the specified regular expression is used to parse the contents of a multi-line log as line N.

items-for-parsing-date-and-time-of-logs

Same as description of "If regexp".

Item Name	Description	Changea bility	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
format_firstline	Specify the first line of the log as a regular expression. The multiline parse plug-in parses multi-line logs. If `multiline` is specified as the type of the parse plug-in, format*N* and format_firstline must be specified. The maximum number of bytes that can be specified in a regular expression is 1023 bytes (excluding delimiters). Regular expressions must be sandwiched between "/" (delimiters). If the delimiter is not used, an error is output.	Changeabl e	Specify the first line of the log as a regular expression according to the format of the log file to be monitored.	--
format*N*	Specify each line of the log as a regular expression. Specifies the format of the multiline log. *N* is an integer from 1 to 20 that creates a list of regular expression formats. The maximum number of bytes that can be specified in a regular expression is 1023 bytes (excluding delimiters). Regular expressions must be sandwiched between "/" (delimiters). If the delimiter is not used, an error is output. If this parameter is not specified, an error is printed when Fluentd is invoked.	Changeabl e	Specify each line of the log as a regular expression according to the format of the log file to be monitored.	--

(Legend) -: Not applicable

- For syslog

```
<parse>
  @type syslog
```

```
    time_type string
    time_format date-and-time-formats
    rfc5424_time_format syslog-date-and-time-format-in-RFC-5424-format
    message_format types-of-syslogs
    with_priority priority-prefix
    parser_type string
    support_colonless_ident presence-or-absence-of-ident-field
    time_key time
    null_empty_string false
    estimate_current_event true
    keep_time_key false
    localtime true
    utc false
  </parse>
```

date-and-time-formats (required)

Same as description of "If regexp". Specify a regular expression to parse the date and time in the log message. If `auto` is specified as *types-of-syslogs*, specify *syslog-date-and-time-format-in-RFC-3164-format*.

syslog-date-and-time-format-in-RFC-3164-format (optional)

Specify a regular expression to parse the date and time of the syslog in RFC-5424 format. Use this parameter only if *types-of-syslogs* is specified to `auto`.

types-of-syslogs (required)

Specify the type of syslog to be analyzed: `rfc3164` (RFC-3164 format), `rfc5424` (RFC-5424 format), or `auto` (both).

priority-prefix (required)

Indicates whether RFC-3164 formatted syslogs contain a priority prefix as `true` or `false`. `false` can be specified only when rfc3164 is specified as *types-of-syslogs*, otherwise it must be specified as `true`.

presence-or-absence-of-ident-field (required)

Specifies whether the RFC-3164-formatted syslog contains the IDENT field as `true` or `false`. `false` can be specified only when rfc3164 is specified as *types-of-syslogs*, otherwise it must be specified as true.

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
time_format	Same as description of "If regexp". If syslog is specified for type and auto is specified for message_format, specifies the RFC-3164 protocol time format. In this case, the RFC-5424 protocol time format is specified in rfc5424_time_format. The RFC-3164 protocol time format is "%b %d %H:%M:%S". If the output is time-stamped in seconds or less, change it to "%b %d %H:%M:%S.%N".	Changeable	Specify the time format as a regular expression according to the format of the log file to be monitored.	--

rfc5424_time_format	Specifies the RFC-5424 protocol time format, up to 256 bytes.
	The following formats are supported:
	`%b:Abbreviated month (Jan,Feb,...)`
	`%d:Day (01~31)`
	`%H: 24-hour clock (00~23)`
	`%M:min(00~59)`
	`%m: Month number (01~12)`
	`%S:sec (00~60 (60 indicates leap second))`
	`%Y: A number representing the year`
		Changeable	Specify the time format according to the format of the log file to be monitored.	--

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent

	`%N: fractional seconds`
	If you specify an incorrect value, a warning message similar to the one shown below may be output to the Fluentd log, and the log may not be monitored.
	`2023-03-24 13:18:27 +0900 [warn]: #0 invalid line found file="/home/ec2-user/fluentd_test/input_log/20230315_log1.txt" line="<16>1 2023-03-24T13:18:27.31+0900 192.168.0.1 fluentd 11111 ID24224 [exampleSDID@20224 iut=\"3\" eventSource=\"Application\" eventID=\"11211\"] Hi, from Fluentd!" error="invalid time format: value = 2023-03-24T13:18:27.31+0900, error_class = ArgumentError, error = string doesn't match"`
	Use this parameter only if the message_format is specified as AUTO. If not specified, the time is parsed and extracted according to the regular expression time format described in *3.15.3(3)(g)Log parsing function (parse plug-in)* of the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.			

message_format	Specifies the protocol format for syslog. You can specify RFC3164, RFC5424, or AUTO. The default is rfc3164. If the monitored syslog is output in RFC5424, specify RFC5424. Also, if the syslog to be monitored is logged using both RFC3164 and RFC5424 protocols, AUTO is specified. If auto is specified, the syslog parsing plug-in uses the message prefix to detect the format. If this parameter is not specified, or if an incorrect value is specified, an error is printed when Fluentd is started.	Changeable	Specify the log format according to the format of the log file to be monitored.	--
with_priority	Indicates whether RFC-3164 formatted syslogs contain a priority prefix as true or false. Specify true if the monitored log has a priority prefix such as [9]. If this parameter is not specified, the Fluentd log may display a warning message similar to the one shown below, and the log may not be monitored. `2023-03-24 14:15:01 +0900 [warn]: #0 pattern not matched: "Mar 24 14:15:01 192.168.0.1 fluentd[11111]: [error] Syslog test"` If a value other than true or false is specified, an error is output when Fluentd is started.	Changeable	Specify according to the format of the log file to be monitored.	--
support_colonless_ident	Specifies whether RFC-3164 formatted syslogs contain the ident field as true or false. Used to monitor logs in RFC3164 format. Specifies false if the monitored log does not contain an ident field in the message. If this parameter is not specified, no error or warning messages are printed, and the monitored log may be parsed in the wrong format. Therefore, it is necessary to check whether JP1 events are issued in a normal format after starting Fluentd and adding logs.	Changeable	Specify according to the format of the log file to be monitored.	--

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
	If a value other than true or false is specified, an error is output when Fluentd is started.			

(Legend) -: Not applicable

- For csv

```
<parse>
  @type csv
  keys array-of-field-names-for-records
  delimiter ,
  parser_type types-of-internal-parsers
  time_key time
  null_empty_string false
  estimate_current_event true
  keep_time_key false
  items-for-parsing-date-and-time-of-logs
</parse>
```

array-of-field-names-for-records (required)

Specifies the field names of the record in the form of an array. One of field names is necessary to be "message" in order to set to MESSAGE of JP1 event. If character strings named "message" is not trimmed, MESSAGE of JP1 event will be empty.

types-of-internal-parsers (required)

Specifies the type of internal parser that parses logs in CSV format.

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
keys	Specify an array of record item names within 256 bytes. If this parameter is not specified, or if an incorrect value is specified, no error or warning message is printed and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.	Changeable	Specify according to the format of the log file to be monitored.	--
parser_type	Specifies the type of internal parser for parsing log lines, either normal or fast. If normal is specified, the Ruby CSV.parse_line method is used. If fast is specified, Fluentd's own lightweight implementation is used. The parser you use is several times faster than usual, but supports only typical patterns. The following formats are supported: # non-quoted value1,value2,value3,value4,value5 # quoted "value1","val,ue2","va,lu,e3","val ue4","" # escaped "message","mes""sage","""message""",,"""""" # mixed message,"mes,sage","me,ssa,ge",mess age,"" If this parameter is not specified, or if an incorrect value is specified, an error is output when Fluentd is started.	Changeable	If the format of the log file to be monitored is in the following format, specify fast. # non-quoted value1,value2,value3,value4,value5 # quoted "value1","val,ue2","va,lu,e3","val ue4","" # escaped "message","mes""sage","""message""",,"""""" # mixed message,"mes,sage","me,ssa,ge",mess age,"" If the format of the log file to be monitored does not	--

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
			match the above format, normal is specified.	

(Legend) -: Not applicable

items-for-parsing-date-and-time-of-logs

Same as description of "If regexp". Specify when array of field names for records has "time".

- For tsv

```
  <parse>
    @type tsv
    keys array-of-field-names-for-records
    delimiter "\t"
    time_key time
    null_empty_string false
    estimate_current_event true
    keep_time_key false
    items-for-parsing-date-and-time-of-logs
  </parse>
```

array-of-field-names-for-records (required)

Specifies the field names of the record in the form of an array.

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
keys	Specify an array of record item names within 256 bytes. If this parameter is not specified, or if an incorrect value is specified, no error or warning message is printed and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.	Changeable	Specify according to the format of the log file to be monitored.	--

(Legend) -: Not applicable

items-for-parsing-date-and-time-of-logs

Same as description of "If regexp". Specify when array of field names for records has "time".

- For ltsv

```
  <parse>
    @type ltsv
    delimiter-between-items delimiter-pattern-between-items
    label_delimiter delimiter-between-label-and-value
    time_key time
    null_empty_string false
    estimate_current_event true
    keep_time_key false
    items-for-parsing-date-and-time-of-logs
  </parse>
```

delimiter-between-items delimiter-pattern-between-items (required)

Specifies the delimiter between items. Specify one of the following:

- When the separator between items is a tab

```
    delimiter "\t"
```

- When the separator between items is one or more blanks

```
    delimiter_pattern /\s+/
```

delimiter-between-label-and-value (required)

Specifies the delimiter between the label and the value.

Item Name	Description	Changeability	JP1/IM - What the user sets on the agent	JP1/IM - Initial value of Agent
delimiter	Specifies the delimiter between items. The only delimiter that can be specified is double-quoted "\t". If either this parameter or delimiter_pattern is specified, or if an incorrect value is specified, no error or warning message is printed and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.	Changeable	Specify according to the format of the log file to be monitored.	--
delimiter_pattern	In an LTSV format file, this is specified when the separator between entries is one or more spaces. The only delimiter that can be specified is "/\s+/". If either this parameter or delimiter is not specified, or if an incorrect value is specified, no error or warning message is output, and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.	Changeable	Specify according to the format of the log file to be monitored.	--
label_delimiter	Specifies the delimiter between the label and the value within 256 bytes. If this parameter is not specified, or if an incorrect value is specified, no error or warning message is printed and the monitored log is parsed in the wrong format. Therefore, after starting Fluentd and adding logs, it is necessary to check whether JP1 events are issued in a normal format.	Changeable	Specify according to the format of the log file to be monitored.	--

(Legend) -: Not applicable

items-for-parsing-date-and-time-of-logs

Same as description of "If regexp". Specify when array of field names for records has "time".

`[Attributes Settings]` section

Serup Attributes of JP1 events to be issued and Attribute value.

log-monitoring-name (mandatory)

Same as description of `[Metric Settings]` section.

event-ID (optional)

Specifies Value to Setup for B. ID property of JP1 event. For details about Value that can be specified, see JP1/Base Operation Manual. The default Value is "00007601" (Event ID used for monitoring text-formatted log file definition file).

If this option is omitted, JP1 events are not issued.

Instead of specifying "`ID` *event-ID*", you can setup *event ID* according to the value of message property by specifying:

```
    ID "${
        if record['message'].match(/regex-1/)
```

```
           'event-ID1'
         elsif record['message'].match(/regex-2/)
           'event-ID2'
         elsif record['message'].match(/regex-3/)
           'event-ID3'
...
         else
           'event-ID4'
         end}"
```

The conditional branch of Ruby determines value of message property and turns setup event ID. In the above cases, if *regex-1* is matched, *event ID* is set to the value as specified in *event-ID-1*. If it doesn't match, it will setup *event-ID-2* if it matches *regex-2*. If none of the matches are compared by the number specified in elsif, else statement setup value specified in *event-ID-4*. to *event ID*. You can specify a maximum of 100 if and elsif statements.

host-name (optional)

Same as description of `[Metric Settings]` section.

If the specification is omitted, the attribute value of JP1_SOURCEHOST is not setup and JP1 event is not add to the correct IM management node.

You can also dynamically setup the canonical host name of the system by doing the following:

```
    JP1_SOURCEHOST ${Socket.gethostname}
```

severity (optional)

Specifies the value to setup for E.SEVERITY property of JP1 event. For details about the value that can be specified, see the *JP1/Base User's Guide*. The default value is "Notice".

If this option is omitted, JP1 events are not issued.

Instead of specifying "`SEVERITY` *severity*", you can setup the severity according to the value of message property by specifying:

```
    SEVERITY "${
         if record['message'].match(/regex-1/)
           'Critical'
         elsif record['message'].match(/regex-2/)
           'Error'
         elsif record['message'].match(/regex-3/)
           'Warning'
...
         else
           'Notice'
         end}"
```

The conditional branch of Ruby determines value of message property and turns setup *severity*. In the above cases, "`Critical`" is setup to *severity* if the *regex-1* is matched. If it doesn't match, it will setup "`Error`" if it matches against *regex-2*. Setup "`Notice`" in else construct to *severity* if elsif matches none of the specified numbers. You can specify up to 100 statements of if and elsif.

IM-management-node-label-name (optional)

Same as description of `[Metric Settings]` section.

If this option is omitted, JP1 events are not issued.

any-attribute-name any-value (optional)

Specify this operand if you want to Add a JP1 event-attribute. For details about Attribute name that can be specified, see JP1/Base Operation Manual.

For Value, you can specify the captured name in the `[Input Settings]` section with the regular expressions to parse the logs.

For example, to capture with the name "NUMBER" and Setup to the property EXIT_CODE, you would specify:

```
EXIT_CODE ${record['NUMBER']}
```

You can Add more than one extended attribute, but no JP1 event is issued if the sum of the sizes of Value that Setup the extended attribute of JP1 event exceeds the limit.

For details about the upper limit of extended attributes, see *4.4.4(5)__transformEvent method*.

`[Inclusion Settings]` section

Specifies the conditions of the log to be monitored in a regular expression. If not specified, all logs are monitored. If an unmonitored log is output, the log is not converted to a JP1 event and is not output to Fluentd log.

In the default Setup, "#" is specified at the beginning of the line and is handled as Comment, so when specifying it, "#" is going to be deleted.

log-monitoring-name (mandatory)

Same as description of `[Metric Settings]` section.

attribute-name-of-JP1-event (optional)

Specifies the attribute name of JP1 event. For example, "`MESSAGE`". If the specification is omitted, error occurs when Fluentd is started.

regular-expression-of-logs-to-monitor (optional)

Specifies a regular expression for the value of the attribute specified by the attribute name of JP1 event. If the value to be match is included, monitoring is performed.

If the specification is omitted, error occurs when Fluentd is started.

You can also specify a logical AND or OR condition for multiple regular expression patterns. For details about how to specify the log data, see *3.15.3(7) Log data extractor (grep plug-in)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`[Exclusion Settings]` section

Specifies the conditions for logs that are not monitored, in regular expressions. If not specified, all logs are monitored. In the default Setup, "#" is specified at the beginning of the line and is handled as Comment, so when specifying it, "#" is going to be deleted.

log-monitoring-name (mandatory)

Same as description of `[Metric Settings]` section.

attribute-name-of-JP1-event (optional)

Specifies the attribute name of JP1 event. For example, "`MESSAGE`".

If the specification is omitted, error occurs when Fluentd is started.

regular-expression-of-logs-to-monitor (optional)

Specifies a regular expression for the value of the attribute specified by *attribute-name-of-JP1-event*. If value to be match is included, monitoring is not performed.

If the specification is omitted, error occurs when Fluentd is started.

You can also specify a logical AND or OR condition for multiple regular expression patterns. For details about how to specify the log data, see *3.15.3(7) Log data extractor (grep plug-in)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`[Forward Settings]` section

Setup the regular expression of the log data to be converted into a JP1 event.

log-monitoring-name (mandatory)

Same as description of `[Metric Settings]` section.

attribute-name-of-JP1-event (optional)

Specifies the attribute name of JP1 event. The default value is "`SEVERITY`".

If the specification is omitted, error occurs when Fluentd is started.

regular-expression-for-logs-that-emit-JP1-events (optional)

Specifies the condition for regular expressions that issue JP1 events for the value of the attribute specified by *attribute-name-of-JP1-event*.

The default value is "`Warning|Error|Critical|Alert|Emergency`" and matches if the value of `SEVERITY` is greater than or equal to `Warning`.

If Value of the attribute contains a Value that Match the condition, the monitored log content is converted to JP1 events and Add to JP1/Base in Integrated manager host. The content of the monitored log is also output to Fluentd log. If you do not Match the condition, JP1 event is not issued and only logged in Fluentd.

If the specification is omitted, Error occurs when Fluentd is started.

In the `[Attributes Settings]` section, "`Notice`" is specified as the default `SEVERITY`. Therefore, the log monitoring result is not output as a JP1 event. It is output only in Fluentd log.

If you want to publish a log with a `SEVERITY` of "`Notice`" as a JP1 event, change the definition as shown in the underlined part:

```
    pattern /Notice|Warning|Error|Critical|Alert|Emergency/
```

Example definition

The following is an example of the condition and definitions for monitoring a textual logging File.

■Conditions

- Path of the logged file to monitor
  `C:\Program Files (x86)\Hitachi\HNTRLib2\spool\*`
- Logging message

```
6027 2022/08/25 17:45:50.219     jbssessionmgr    000018EC 00000FCC KAVA14
97-I            jp1admin user has Login
```

- Log messages to monitor
  Monitor the logging message where message ID starts with KAVA.
- Value to setup to MESSAGE
  Setup message ID or later text in the logging message.
- Value to setup to SEVERITY
  Setup value according to severity of message ID.
- Value to setup to any attribute name
  Setup the process-name (jbssessionmgr) contained in the log message to attribute name PROCESS_NAME.

■Definitions

```
<worker 0>
## [Metric Settings]
<source>
  @type exec
  command "echo {}"
  <parse>
    @type json
  </parse>
  run_interval 60s
  tag jpc_ima_metrics.tail.user_app_log
</source>

<filter jpc_ima_metrics.tail.user_app_log>
  @type record_transformer
  enable_ruby true
  <record>
    __name__ fluentd_logtrap_running
    instance hostA
    jp1_pc_nodelabel UserApplication
    jp1_pc_category applicationServer
    jp1_pc_logtrap_defname user_app_log_tail
    jp1_pc_trendname fluentd
    job jpc_fluentd
    jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
    jp1_pc_addon_program JPC Fluentd
  </record>
</filter>
</worker>
<worker 1>
## [Input Settings]
<source>
  @type tail
  tag tail.user_app_log
  path C:/Program Files (x86)/Hitachi/HNTRLib2/spool/*
  follow_inodes true
  refresh_interval 60
  skip_refresh_on_startup false
  read_from_head false
  encoding "UTF-8"
  from_encoding "Shift_JIS"
  read_lines_limit 1000
  read_bytes_limit_per_second -1
  pos_file ../data/fluentd/tail/user_app_log.pos
  path_key tailed_path
  rotate_wait 5s
  enable_watch_timer false
  enable_stat_watcher true
  open_on_every_update false
  emit_unmatched_lines false
  ignore_repeated_permission_error false
  <parse>
    @type regexp
    expression /^([^ ]* +(?<time>[^ ]* [^ ]*) +(?<PROCESS>[^ ]*) +[^ ]* +[^
]* +(?<message>.*))$/
    time_key time
    null_empty_string false
    estimate_current_event true
    keep_time_key false
    localtime true
    utc false
  </parse>
</source>
```

```
## [Attributes Settings]
<filter tail.user_app_log>
  @type record_transformer
  enable_ruby true
  auto_typecast true
  renew_record true

  <record>
    ID 00007601
    MESSAGE ${record["message"]}
    JP1_SOURCEHOST hostA
    JPC_LOG_TIME ${time.utc.to_i}
    PRODUCT_NAME /HITACHI/JP1/JPCCS2/LOGTRAP/UserApplication
    PPNAME /HITACHI/JP1/JPCCS2/LOGTRAP
    SEVERITY "${
         if record['message'].match(/^KAVA[1-9]*-E/)
           'Error'
         elsif record['message'].match(/^KAVA[1-9]*-W/)
           'Warning'
         elsif record['message'].match(/^KAVA[1-9]*-I/)
           'Information'
         else
           'Notice'
         end}"
    PLATFORM ${ if RUBY_PLATFORM.downcase =~ /mswin(?!ce)|mingw|cygwin|bccwi
n/; 'NT'; else 'UNIX'; end }
    OBJECT_TYPE LOGFILE
    OBJECT_NAME ${record['tailed_path']}
    ROOT_OBJECT_TYPE LOGFILE
    ROOT_OBJECT_NAME ${record['tailed_path']}
    JP1_TRAP_NAME ${tag_parts[1]}
    JPC_NODELABEL UserApplication
    PROCESS_NAME ${record['PROCESS']}
  </record>
</filter>

## [Inclusion Settings]
<filter tail.user_app_log>
  @type grep
  <regexp>
    key MESSAGE
    pattern /^KAVA[1-9]*-(I|W|E)/
  </regexp>
</filter>

## [Exclusion Settings]
#<filter tail.user_app_log>
#  @type grep
#  <exclude>
#    key
#    pattern //
#  </exclude>
#</filter>

## [Forward Settings]
<match tail.user_app_log>
  @type rewrite_tag_filter
  <rule>
    key SEVERITY
    pattern /Warning|Error|Critical|Alert|Emergency/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key SEVERITY
    pattern /.*/
    tag ${tag}.outputlog
  </rule>
</match>

<filter /tail\.user_app_log\.(jp1event|outputlog)/>
  @type record_transformer
  enable_ruby true
  auto_typecast true
  renew_record true
  <record>
    eventId ${record['ID']}
    xsystem true
    message ${record['MESSAGE']}
    attrs ${record}
  </record>
  remove_keys $.attrs.ID
  remove_keys $.attrs.MESSAGE
</filter>
</worker>
```

Windows event log monitoring definition file (fluentd_@@trapname@@_wevt.conf.template)

Format

```
<worker 0>
## [Metric Settings]
<source>
  @type exec
  command "echo {}"
  <parse>
    @type json
  </parse>
  run_interval 60s
  tag jpc_ima_metrics.wevt.log-monitoring-name
</source>

<filter jpc_ima_metrics.wevt.log-monitoring-name>
  @type record_transformer
  enable_ruby true
  auto_typecast false

  <record>
    __name__ fluentd_logtrap_running
    instance host-name
    jp1_pc_nodelabel IM-management-node-label-name
    jp1_pc_category category-ID
    jp1_pc_logtrap_defname log-monitoring-name_wevt
    jp1_pc_trendname fluentd
    job jpc_fluentd
    jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
    jp1_pc_addon_program JPC Fluentd
  </record>
</filter>
</worker>
<worker worker-id>
## [Input Settings]
<source>
  @type windows_eventlog2
  tag wevt.log-monitoring-name
  channels log-type
  read_interval 2s
  <storage>
    @type local
    path ../data/fluentd/wevt/log-monitoring-name
    mode 0600
    dir_mode 0700
    pretty_print false
  </storage>
  read_existing_events false
  render_as_xml false
  rate_limit -1
  preserve_qualifiers_on_hash true
  read_all_channels false
  event_query *
</source>
```

```
## [Attributes Settings]
<filter wevt.log-monitoring-name>
  @type record_transformer
  enable_ruby true
  auto_typecast false
  renew_record false
  <record>
    ID event-ID
    JP1_SOURCEHOST host-name
    JPC_NODELABEL IM-management-node-label-name
    JP1_TRAP_NAME log-monitoring-name
#    OS_VERSION OS-version
  </record>
</filter>

## [Inclusion Settings]
#<filter wevt.log-monitoring-name>
#  @type grep
#  <regexp>
#    key attribute-name-of-JP1-event
#    pattern /regular-expressions-for-logs-to-monitor/
#  </regexp>
#</filter>

## [Exclusion Settings]
#<filter wevt.log-monitoring-name>
#  @type grep
#  <exclude>
#    key attribute-name-of-JP1-event
#    pattern /regular-expression-for-logs-not-to-monitor/
#  </exclude>
#</filter>

## [Forward Settings]
<match wevt.log-monitoring-name>
  @type rewrite_tag_filter
  <rule>
    key attribute-name-of-JP1-event
    pattern /regular-expression-for-logs-that-emit-JP1-events/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key MESSAGE
    pattern /.+/
    tag ${tag}.outputlog
  </rule>
</match>

<filter /wevt\.log-monitoring-name\.(jp1event|outputlog)/>
  @type record_transformer
  enable_ruby true
  auto_typecast true
  renew_record true
  <record>
    eventId ${record['ID']}
    xsystem true
    message ${record['MESSAGE']}
    attrs ${record}
  </record>

  remove_keys $.attrs.ID
  remove_keys $.attrs.MESSAGE
</filter>
</worker>
```

File

`fluentd_@@trapname@@_wevt.conf.template`

`fluentd_@@trapname@@_wevt.conf.template.model` (model file)

Storage directory

■Integrated agent host

- For a physical host (Definition file and model file)
  Agent-path`\conf\`
- For a logical host (Definition file)
  shared-folder`\jp1ima\conf\`

Description

Definition file for monitoring Windows event logs.

Copy the template (`fluentd_@@trapname@@_wevt.conf.template`) and change file designation of Copy destination to `fluentd_`*log-monitoring-name*`_wevt.conf` to use it. For details on the location of `fluentd_`*log-monitoring-name*`_wevt.conf`, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. File name must be unique within the monitoring agent host. The characters that can be used for *log-monitoring-name* are alphanumeric characters, hyphens, and underscores, and the length of the character string is 1 to 30 characters. Create this file for each application you want to monitor.

JP1/IM - Agent creates a IM managed node for setup SID of monitoring target according to value specified in *IM-management-node-label-name* in the monitoring definition file. If *IM-management-node-label-name* is the same even if it is another monitoring definition file, only one IM management node is created.

Windows Event Log Monitor feature reads this File and analyzes the log information that the application has written to Windows Event Log. If conditions are specified for the analyzed information and the conditions are met, you can Setup the information to be converted to JP1 events or output to Fluentd logging File. For JP1 event to be issued, see *3.2.3(3) JP1 event to be issued by monitoring Windows event log*.

Lines that begin with a "`#`" are treated as comments and do not affect programming behavior.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

When the definitions are applied

This information is reflected in Fluentd operation when Fluentd serviceis Restart.

If add, delete of a definition file, or value in `[Metric Settings]` section is changed, the change is reflected in tree view of the Integrated Operation Viewer windows.

For details about application method, see *1.21.2(16) Creation and import of IM management node tree data (for Windows) (mandatory)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Information that is specified

`<worker>` directive

Same as `<worker>` directive of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

worker-id (optional)

Description	Changeability	What You Setup in Your JP1/IM - Agent	JP1/IM - Agent Defaults Value
Same as *worker-id* of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.	Can be changed	Same as *worker-id* of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.	2

`[Metric Settings]` section

See the description of the `[Metric Settings]` section in *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

`[Input Settings]` section

Specifies the event log type to monitor.

log-monitoring-name (mandatory)

Same as *log-monitoring-name* in the `[Metric Settings]` section of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

log-type (mandatory)

Specifies the event log type to be monitored as a comma-separated string. It is 256 bytes or less. The default value for JP1/IM - Agent is "`application, system`".

For details about the log type that can be specified, see *3.15.3(4)(a) Types of logs that can be monitored* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`[Attributes Settings]` section

Setup attributes and attribute value of JP1 events to be issued.

log-monitoring-name (mandatory)

Same as *log-monitoring-name* in the `[Metric Settings]` section of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

event-ID (optional)

Same as the event ID in the `[Attributes Settings]` section of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

host-name (optional)

Same as *host-name* in the `[Attributes Settings]` section of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

IM-management-node-label-name (optional)

Same as *IM-management-node-label-name* in the `[Attributes Settings]` section of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

OS-version (optional)

Specifies the number of the major version for Windows if you want JP1 event to add the attributes of `OS_VERSION`. In the default setup, "`#`" is specified at the beginning of the line, and it is handled as comment, so when specifying it, delete "`#`".

`[Inclusion Settings]` section

See the description of the `[Inclusion Settings]` section in *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

`[Exclusion Settings]` section

See the description of the `[Exclusion Settings]` section in *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

`[Forward Settings]` section

See the description of the `[Forward Settings]` section in *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

Example definition

In the following example, monitoring is performed when the log type is "`application`" and the source is "`JP1/IM-Manager`", and a JP1 event is issued when the event level is "`Warning`" or higher.

```
<worker 0>
## [Metric Settings]
<source>
  @type exec
  command "echo {}"
  <parse>
    @type json
  </parse>
  run_interval 60s
  tag jpc_ima_metrics.wevt.user_app_log
</source>

<filter jpc_ima_metrics.wevt.user_app_log>
  @type record_transformer
  enable_ruby true

  <record>
    __name__ fluentd_logtrap_running
    instance hostA
    jp1_pc_nodelabel UserApplication
    jp1_pc_category applicationServer
    jp1_pc_logtrap_defname user_app_log_wevt
    jp1_pc_trendname fluentd
    job jpc_fluentd
    jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
    jp1_pc_addon_program JPC Fluentd
  </record>
</filter>
</worker>
<worker 2>
```

```
## [Input Settings]
<source>
  @type windows_eventlog2
  tag wevt.user_app_log
  channels application
  read_interval 2
  preserve_qualifiers_on_hash true
  <storage>
    @type local
    path ../data/jp1ima/data/fluentd/wevt/user_app_log
  </storage>
  read_from_head false
  render_as_xml false
  rate_limit -1
  preserve_qualifiers_on_hash true
  event_query *
</source>

## [Attributes Settings]
<filter wevt.user_app_log>
  @type record_transformer
  enable_ruby true
  renew_record false
  <record>
    ID 00007602
    JP1_SOURCEHOST hostA
    JPC_NODELABEL UserApplication
    OS_VERSION 10
  </record>
</filter>

## [Inclusion Settings]
<filter wevt.user_app_log>
  @type grep
  <regexp>
    key PRODUCT_NAME
    pattern /JP1\/IM-M$/
  </regexp>
</filter>

## [Exclusion Settings]
#<filter wevt.user_app_log>
#  @type grep
#  <exclude>
#    key
#    pattern //
#  </exclude>
#</filter>

## [Forward Settings]
<match wevt.user_app_log>
  @type rewrite_tag_filter
  <rule>
    key SEVERITY
    pattern /Warning|Error|Critical|Alert|Emergency/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key SEVERITY
    pattern /.*/
    tag ${tag}.outputlog
  </rule>
</match>

<filter /wevt\.user_app_log\.(jp1event|outputlog)/>
  @type record_transformer
  enable_ruby true
  auto_typecast true
  renew_record true
  <record>
    eventId ${record['ID']}
    xsystem true
    message ${record['MESSAGE']}
    attrs ${record}
  </record>

  remove_keys $.attrs.ID
  remove_keys $.attrs.MESSAGE
</filter>
</worker>
```

Sample file of system log information monitoring definition file for SAP system (fluentd_sap_syslog_tail.conf)

Format

This is similar to the format of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

A definition example for monitoring system log information of an SAP system using the monitor function of a log file in text format under the following conditions is provided as a sample file.

- Conditions

- Monitored log file
  - Monitors the log file of the command that extracts the system log information of SAP system.
  - The language setting for the command execution environment is Japanese, and the character encoding is SJIS. If the character code of the log file to be monitored is not SJIS, change the character encoding specified in the from encoding of [Input Settings] (when operating in a Linux environment, it is necessary to change the character code specified to UTF-8).
- Monitoring name

  It is called "sap_syslog".
- Example log messages

  Monitor the logs output in the system log message record with the default layout.

  The default layout is as follows. For details about the extractable fields and specifications of the command, see *jr3slget*.

  ```
  <TIME><INSTANCE><USER><PROGRAM><MSGNO><MSGTEXT>
  ```

  The following is an example of the log message that is output.

  ```
  13:58:04o246bci_SD5_00      SAPSYS      SAPMSSY1D01 Transaction canceled 0
  0 152 ( )  (omitted)
  ```

  # The length of <MSGTEXT> is 255 bytes.

  The above log message is structured for each field as follows.

Fielding ID	Field	Value
<TIME>	Message recording time	`13:58:04`
<INSTANCE>	Server that recorded the message	`o246bci_SD5_00`
<USER>	User who recorded the message	`SAPSYS`
<PROGRAM>	Program that recorded the message	`SAPMSSY1`
<MSGNO>	Message number	`D01`
<MSGTEXT>	Message text	`Transaction canceled 00 152 ( )`

- Log messages to monitor

  Monitor all logs. The message records in the system log are cut out for each field, and each is set as an attribute of the JP1 event. The correspondence between each field and the name when cropped by the regular expression named capture function and the extended attribute of the JP1 event is as follows.

Field ID	Name to cut with regular expression	JP1 event attributes	What to set
<TIME>	sap_time	Not specified.	--
<INSTANCE>	instance		
<USER>	user		
<PROGRAM>	program		
<MSGNO>	msgno		
<MSGTEXT>	message	MESSAGE	Stores the value of the field as is.

Legend: -- : Not applicable

- Value to set for SEVERITY
  Set "Notice".
- Log data to convert to JP1 events
  Matches when SEVERITY is greater than or equal to "Warning". Because "Notice" is specified for SEVERITY, JP1 event is not issued and is output only to Fluentd logging.
- Label name of IM management node
  SAP Syslog

- Definition example

```
<worker 0>
## [Metric Settings]
  <source>
    @type exec
    command "echo {}"
    <parse>
      @type json
    </parse>
    run_interval 60s
    tag jpc_ima_metrics.tail.sap_syslog
  </source>

  <filter jpc_ima_metrics.tail.sap_syslog>
    @type record_transformer
    enable_ruby true
    auto_typecast false
    <record>
      __name__ fluentd_logtrap_running
      instance @@sap_instancename@@
      jp1_pc_nodelabel SAP Syslog
      jp1_pc_category enterprise
      jp1_pc_logtrap_defname sap_syslog_tail
      jp1_pc_trendname fluentd
      job jpc_fluentd
      jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
      jp1_pc_addon_program JPC Fluentd
    </record>
  </filter>
</worker>

<worker 3>
```

```
## [Input Settings]
  <source>
    @type tail
    tag tail.sap_syslog
    path @@sap_logpath@@
    follow_inodes true
    refresh_interval 60
    skip_refresh_on_startup false
    read_from_head false
    encoding "UTF-8"
    from_encoding "Shift_JIS"
    read_lines_limit 1000
    read_bytes_limit_per_second -1
    pos_file ../data/fluentd/tail/sap_syslog.pos
    path_key tailed_path
    rotate_wait 5s
    enable_watch_timer false
    enable_stat_watcher true
    open_on_every_update false
    emit_unmatched_lines false
    ignore_repeated_permission_error false
    <parse>
      @type regexp
      expression /^(?<sap_time>.{8})(?<instance>.{20})(?<user>.{12})(?<progr
am>.{8})(?<msgno>.{3})(?<message>.*)$/
      time_key time
      null_empty_string false
      estimate_current_event true
      keep_time_key false
      localtime true
      utc false
    </parse>
  </source>

## [Attributes Settings]
  <filter tail.sap_syslog>
    @type record_transformer
    enable_ruby true
    auto_typecast false
    renew_record true

    <record>
      ID 00007601
      MESSAGE ${record["message"]}
      JP1_SOURCEHOST @@sap_instancename@@
      JPC_LOG_TIME ${time.utc.to_i}
      PRODUCT_NAME /HITACHI/JP1/JPCCS2/LOGTRAP/SAP Syslog
      PPNAME /HITACHI/JP1/JPCCS2
      SEVERITY Notice
      PLATFORM ${ if RUBY_PLATFORM.downcase =~ /mswin(?!ce)|mingw|cygwin|bcc
win/; 'NT'; else 'UNIX'; end }
      OBJECT_TYPE LOGFILE
      OBJECT_NAME ${record['tailed_path']}
      ROOT_OBJECT_TYPE LOGFILE
      ROOT_OBJECT_NAME ${record['tailed_path']}
      JP1_TRAP_NAME ${tag_parts[1]}
      JPC_NODELABEL SAP Syslog
    </record>
  </filter>

## [Inclusion Settings]
#<filter tail.sap_syslog>
#    @type grep
#    <regexp>
#      key nil
#      pattern nil
#     </regexp>
#  </filter>

## [Exclusion Settings]
#  <filter tail.sap_syslog>
#    @type grep
#    <exclude>
#      key nil
#      pattern nil
#    </exclude>
#  </filter>

## [Forward Settings]
  <match tail.sap_syslog>
    @type rewrite_tag_filter
    <rule>
      key SEVERITY
      pattern /Warning|Error|Critical|Alert|Emergency/
      tag ${tag}.jp1event
    </rule>
    <rule>
      key SEVERITY
      pattern /.*/
      tag ${tag}.outputlog
    </rule>
  </match>

  <filter /tail\.sap_syslog\.(jp1event|outputlog)/>
    @type record_transformer
    enable_ruby true
    auto_typecast true
    renew_record true
    <record>
      eventId ${record['ID']}
      xsystem true
      message ${record['MESSAGE']}
      attrs ${record}
    </record>
    remove_keys $.attrs.ID
    remove_keys $.attrs.MESSAGE
  </filter>
</worker>
```

File

`fluentd_sap_syslog_tail.conf`

Storage directory

- Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\sample\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/sample/`

Description

Sample file of the definition file for monitoring system log information of SAP system.

Copy sample file (`fluentd_sap_syslog_tail.conf`) and change the file name of the copy destination to `fluentd_log monitor name_tail.conf` if required. For the location of the files, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. This definition file is created for each script specified by Script exporter configuration file (jpc_script_exporter.yml).

Lines that start with a "#" are treated as comments and do not affect program operation.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When Fluentd service restarts, it is reflected in Fluentd operation.

When a definition file is added or deleted, or the value in the [Metric Settings] section is changed, the changes are reflected in integrated operation viewer tree view.

For details about how to import trees, see *1.21.2(16) Creation and import IM management node tree data (for Windows) (mandatory)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Information that is specified

See the description of *Information that is specified* in *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

If a user wants to use this sample file, the following settings must be changed according to the user environment.

Setting item	Initial value	Setting contents
Path of the monitored log file	`@@sap_logpath@@`	Specify the path of the text file specified by the user in the environment parameters file to output the results of extracting the system log information of the SAP system.
SAP instance name from which you want to extract system log information	`@@sap_instancename@@`	Specify the name of the SAP instance to output the results of extracting system log information from the SAP system.

In addition, JP1 event is issued when a match occurs when SEVERITY is greater than or equal to "Warning". In this sample, SEVERITY is always set to "Notice", so JP1 events are not emitted, but only output to the Fluentd log. When outputting log monitoring results as JP1 events, change the definition as shown in the underlined part below.

```
## [Forward Settings]
<match tail.sap_syslog>
  @type rewrite_tag_filter
  <rule>
    key SEVERITY
    pattern /Notice|Warning|Error|Critical|Alert|Emergency/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key SEVERITY
    pattern /.*/
    tag ${tag}.outputlog
  </rule>
</match>
```

Sample file of CCMS alert information monitoring definition file for SAP system (fluentd_sap_alertlog_tail.conf)

Format

This is similar to the format of *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)*.

A definition example for monitoring CCMS alert information of an SAP system using the monitor function of a log file in text format under the following conditions is provided as a sample file.

- Conditions

- Monitored log file
    - Monitors the log file of the command that extracts CCMS alert information of SAP system.
    - The language setting for the command execution environment is Japanese, and the character encoding is SJIS. If the character code of the log file to be monitored is not SJIS, change the character encoding specified in the from encoding of [Input Settings] (when operating in a Linux environment, it is necessary to change the character code specified to UTF-8).
- Monitoring name

  It is called "sap_alertlog".
- Example log messages

  Monitor the logs that are printed in CCMS alert record with the default layout.

  The default layout is as follows: For details about the extractable fields and specifications of the command, see *jr3alget*.

```
<ALERT_DATE><ALERT_TIME><MTSYSID><MTMCNAME><OBJECTNAME><FIELDNAME><VALUE><
SEVERITY><MSG>
```

  The following is an example of the log message that is output.

```
20231219041721NWE     Background                              Backgroun
dService                       SystemWideFreeBPWP
3          50         0 WPs > 2 WPs the current value exceeds the thres
hold  (omitted)
```

  # The length of <MSG> is 255 bytes.

  The above log message is structured for each field as follows.

Fielding ID	Field	Value
<ALERT_DATE>	Alerting Date (YYYYMMDD)	`20231219`
<ALERT_TIME>	Alerting time (HHMMSS)	`041721`
<MTSYSID>	Name of SAP system	`NWE`
<MTMCNAME>	Monitor context name	`Background`
<OBJECTNAME>	Monitor object name	`BackgroundService`
<FIELDNAME>	MTE abbreviation	`SystemWideFreeBPWP`
<VALUE>	Warning value	`3`
<SEVERITY>	Severity	`50`

Fielding ID	Field	Value
<MSG>	Translated messages	`0 WPs > 2 WPs` the current value exceeds the threshold

- Log messages to monitor

  Monitor all logs. Excludes the message records in the system log field by field, and sets the translated message and warning value as the JP1 event message and severity, respectively. The correspondence between each field and the name when cropped by the regular expression named capture function and the extended attribute of the JP1 event is as follows.

Field ID	Name to cut with regular expression	JP1 event attributes	What to set
<ALERT_DATE>	alertdate	Not specified.	--
<ALERT_TIME>	alerttime		
<MTSYSID>	mtsysid		
<MTMCNAME>	mtmcname		
<OBJECTNAME>	objectname		
<FIELDNAME>	fieldname		
<VALUE>	value	SEVERITY	`Stores the severity according to the <VALUE> setting.` • If it is 0: Debug • If it is 1: Information • If it is 2: Warning • If it is 3: Error • Otherwise: Notice
<SEVERITY>	severity	Not specified.	--
<MSG>	message	MESSAGE	Stores the value of the field as-is.

Legend: -- : Not applicable

- Log data to convert to JP1 events

  Matches when SEVERITY is greater than or equal to Warning. If SEVERITY is specified as "Debug", "Information", or "Notice", no JP1 events are issued and only logged to Fluentd.

  Label name of IM management node

  SAP CCMS Alert

- Definition example

```
<worker 0>
## [Metric Settings]
  <source>
    @type exec
    command "echo {}"
    <parse>
      @type json
    </parse>
    run_interval 60s
    tag jpc_ima_metrics.tail.sap_alertlog
  </source>
  <filter jpc_ima_metrics.tail.sap_alertlog>
    @type record_transformer
    enable_ruby true
    auto_typecast false
    <record>
      __name__ fluentd_logtrap_running
      instance @@sap_instancename@@
      jp1_pc_nodelabel SAP CCMS Alert
      jp1_pc_category enterprise
      jp1_pc_logtrap_defname sap_alertlog_tail
      jp1_pc_trendname fluentd
      job jpc_fluentd
      jp1_pc_nodelabel_fluentd Log trapper(Fluentd)
      jp1_pc_addon_program JPC Fluentd
    </record>
  </filter>
</worker>

<worker 4>
## [Input Settings]
  <source>
    @type tail
    tag tail.sap_alertlog
    path @@sap_logpath@@
    follow_inodes true
    refresh_interval 60
    skip_refresh_on_startup false
    read_from_head false
    encoding "UTF-8"
    from_encoding "Shift_JIS"
    read_lines_limit 1000
    read_bytes_limit_per_second -1
    pos_file ../data/fluentd/tail/sap_alertlog.pos
    path_key tailed_path
    rotate_wait 5s
    enable_watch_timer false
    enable_stat_watcher true
    open_on_every_update false
    emit_unmatched_lines false
    ignore_repeated_permission_error false
    <parse>
      @type regexp
      expression /^(?<alert_date>.{8})(?<alert_time>.{6})(?<mtsysid>.{8})(?<
mtmcname>.{40})(?<objectname>.{40})(?<fieldname>.{40})(?<value>.{11})(?<seve
rity>.{11})(?<message>.*)$/
      time_key time
      null_empty_string false
      estimate_current_event true
      keep_time_key false
      localtime true
      utc false
    </parse>
  </source>

## [Attributes Settings]
  <filter tail.sap_alertlog>
    @type record_transformer
    enable_ruby true
    auto_typecast false
    renew_record true

    <record>
      ID 00007601
      MESSAGE ${record["message"]}
      JP1_SOURCEHOST @@sap_instancename@@
      JPC_LOG_TIME ${time.utc.to_i}
      PRODUCT_NAME /HITACHI/JP1/JPCCS2/LOGTRAP/SAP CCMS Alert
      PPNAME /HITACHI/JP1/JPCCS2
#       SEVERITY Notice
      SEVERITY "${
           if record['value'].match(/3/)
             'Error'
           elsif record['value'].match(/2/)
             'Warning'
           elsif record['value'].match(/1/)
             'Information'
           elsif record['value'].match(/0/)
             'Debug'
           else
             'Notice'
           end}"
      PLATFORM ${ if RUBY_PLATFORM.downcase =~ /mswin(?!ce)|mingw|cygwin|bcc
win/; 'NT'; else 'UNIX'; end }
      OBJECT_TYPE LOGFILE
      OBJECT_NAME ${record['tailed_path']}
      ROOT_OBJECT_TYPE LOGFILE
      ROOT_OBJECT_NAME ${record['tailed_path']}
      JP1_TRAP_NAME ${tag_parts[1]}
      JPC_NODELABEL SAP CCMS Alert
    </record>
  </filter>

## [Inclusion Settings]
#<filter tail.sap_alertlog>
#    @type grep
#    <regexp>
#      key nil
#      pattern nil
#    </regexp>
#  </filter>

## [Exclusion Settings]
#  <filter tail.sap_alertlog>
#    @type grep
#    <exclude>
#      key nil
#      pattern nil
#    </exclude>
#  </filter>

## [Forward Settings]
  <match tail.sap_alertlog>
    @type rewrite_tag_filter
    <rule>
      key SEVERITY
      pattern /Warning|Error|Critical|Alert|Emergency/
      tag ${tag}.jp1event
    </rule>
    <rule>
      key SEVERITY
      pattern /.*/
      tag ${tag}.outputlog
    </rule>
  </match>

  <filter /tail\.sap_alertlog\.(jp1event|outputlog)/>
    @type record_transformer
    enable_ruby true
    auto_typecast true
    renew_record true
    <record>
      eventId ${record['ID']}
      xsystem true
      message ${record['MESSAGE']}
      attrs ${record}
    </record>
    remove_keys $.attrs.ID
    remove_keys $.attrs.MESSAGE
  </filter>
</worker>
```

File

`fluentd_sap_alertlog_tail.conf`

Storage directory

- Integrated agent host

In Windows

- For a physical host
  Agent-path`\conf\sample\`

In Linux:

- For a physical host:
  `/opt/jp1ima/conf/sample/`

Description

Sample file of the definition file used to monitor CCMS alerting for SAP system.

Copy sample file (fluentd_sap_alertlog_tail.conf) and change the file name of the copy destination to fluentd_Log monitoring name_tail.conf if required. For the location of the files, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. This definition file is created for each script specified by Script exporter configuration file (jpc_script_exporter.yml).

Lines that start with a "#" are treated as comments and do not affect program operation.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When Fluentd service restarts, it is reflected in Fluentd operation.

When a definition file is added or deleted, or the value in the [Metric Settings] section is changed, the changes are reflected in integrated operation viewer tree view.

For the reflection method, see *1.21.2(16) Creation and import IM management node tree data (for Windows) (mandatory)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

Information that is specified

See the description of *Information that is specified* in Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template).

If you want to use this sample file, you must modify the following settings to suit your needs.

Setting item	Initial value	Information that is specified
Path of the monitored log file	`@@sap_logpath@@`	Specify the path of the text file specified by the user in the environment parameter setting file to output the extraction result of CCMS alert information of the SAP system.
SAP instance name from which you want to extract CCMS alert information	`@@sap_instancename@@`	Specify the SAP instance name to output the extraction result of CCMS alert information of the SAP system.

In addition, JP1 event is issued when a match occurs when SEVERITY is greater than or equal to "Warning". If SEVERITY is specified as "Notice", "Debug", or "Information", no JP1 events are issued and only logged to Fluentd. If SEVERITY is "Notice", "Debug", or "Information" and log monitoring results are to be output as JP1 events, change the definition as shown in the underlined part below.

```
## [Forward Settings]
<match tail.sap_alertlog>
  @type rewrite_tag_filter
  <rule>
    key SEVERITY
    pattern /Notice|Debug|Information|Warning|Error|Critical|Alert|Emergenc
y/
    tag ${tag}.jp1event
  </rule>
  <rule>
    key SEVERITY
    pattern /.*/
    tag ${tag}.outputlog
  </rule>
</match>
```

Environment parameters file for jr3slget command (jr3slget.ini)

If you specify an environment parameters file as an argument in the `jr3slget` command, the command extracts the system log information of the SAP system based on the settings in the file.

You create this environment parameters file as a text file.

Setup procedure

To set up the environment parameters file:

1. Before you edit the environment parameters file, make sure that the `jr3slget` command is not running.

2. To create a new environment parameters file, copy the sample environment parameters file under the name `jr3slget.ini`.

   This `jr3slget.ini` becomes the default environment parameters file. The sample file of environment parameters file is as follows:

   ■Integrated agent host

   In Windows:

   - For a physical host:

     Folder-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Windows*`\sap_windows\command\agtm\evtrap\jr3slget.ini.sample`

     #: *Agent-path*`\options\sap_windows_`*VVRRSS*`.zip`

   In Linux:

   - For a physical host:

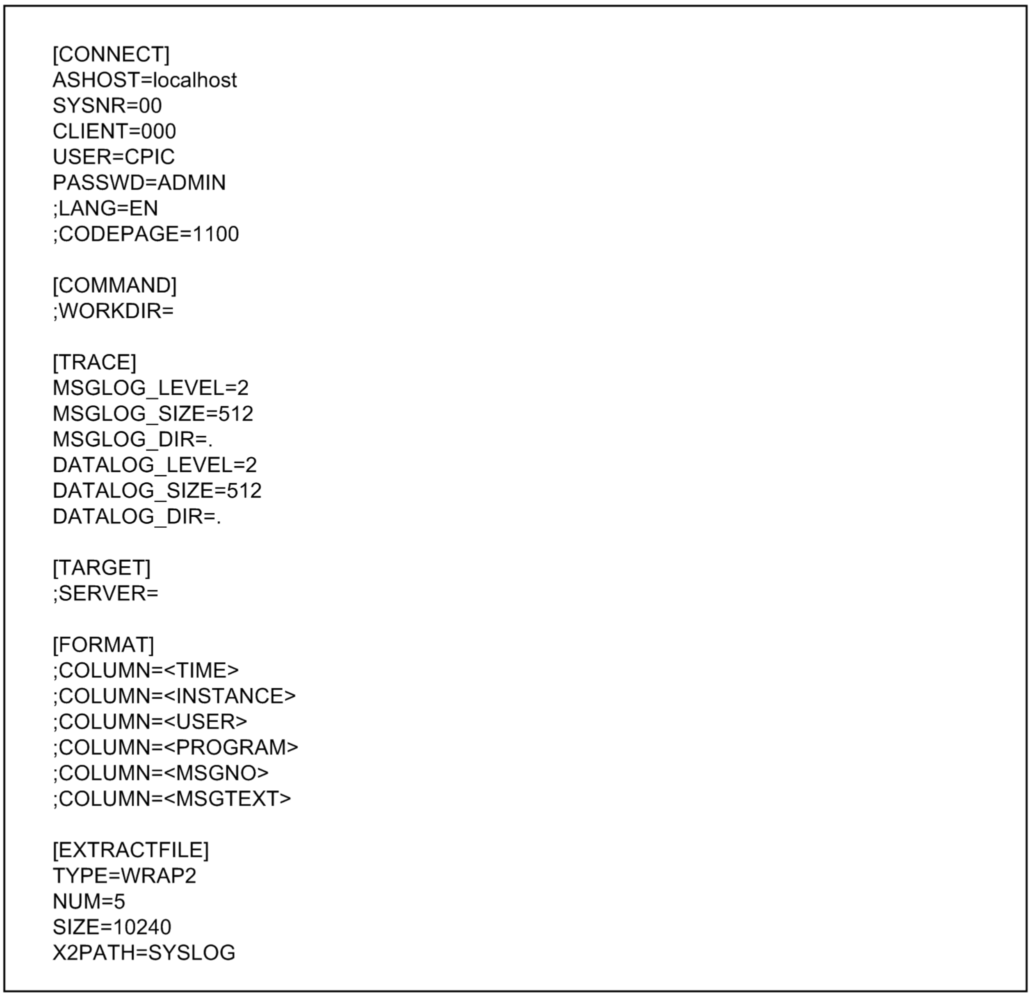
     Directory-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Linux*`/sap_linux/command/agtm/evtrap/jr3slget.ini.sample`

     #: `/opt/jp1ima/options/sap_linux_`*VVRRSS*`.tar.gz`

3. Open the `jr3slget.ini` file.

4. Edit the settings.

   The settings in the default environment parameters file are as follows; for details about the settings, see *Settings*:



```
[CONNECT]
ASHOST=localhost
SYSNR=00
CLIENT=000
USER=CPIC
PASSWD=ADMIN
;LANG=EN
;CODEPAGE=1100

[COMMAND]
;WORKDIR=

[TRACE]
MSGLOG_LEVEL=2
MSGLOG_SIZE=512
MSGLOG_DIR=.
DATALOG_LEVEL=2
DATALOG_SIZE=512
DATALOG_DIR=.

[TARGET]
;SERVER=

[FORMAT]
;COLUMN=<TIME>
;COLUMN=<INSTANCE>
;COLUMN=<USER>
;COLUMN=<PROGRAM>
;COLUMN=<MSGNO>
;COLUMN=<MSGTEXT>

[EXTRACTFILE]
TYPE=WRAP2
NUM=5
SIZE=10240
X2PATH=SYSLOG
```

In the case of an item that begins with a semicolon (`;`), the setting is disabled by default, because the semicolon indicates that it is a comment line. To enable the setting, remove the semicolon.

5. Save the environment parameters file.

   By specifying the `-cnf` option in the `jr3slget` command, you can extract the system log information of the SAP system based on the settings in the environment parameters file.

Settings

Specify the settings in the environment parameters file in the following format:

```
[section]
label=value
label=value
...
...
[section]
label=value
label=value
```

Notes

- Do not specify any unneeded characters, such as spaces at the beginning of a line or before and after an equals sign (=).
- The values specified in *section* and *label* are not case-sensitive.

- A line beginning with a semicolon (;) is treated as a comment.

The following tables describe the contents of each section in the environment parameters file. In a table, the *Argument* column indicates the argument that is specified in the jr3slget command, if applicable. N/A means that the item cannot be specified with the command.

CONNECT section

The CONNECT section specifies information needed to establish RFC connection with the SAP system at the time of command execution.

Table 2–98: Values permitted in the CONNECT section

Label	Description	Permitted values	Default value	Argument
ASHOST	Host name of the connection-target application server (which can be verified by transaction code SM51)	1-100 single-byte alphanumeric characters in one of the following formats: • Host name specified in the hosts file • IP address • SAP router address	localhost	-h
SYSNR	System number that can be identified by the connection-target application server host	0-99	00	-s
CLIENT	User's client name used for establishing connection	0-999	000	-c
USER	User name used for establishing connection#1	1-12 single-byte alphanumeric characters	CPIC	-u
PASSWD	User's password used for establishing connection#2	1-8 single-byte characters#3	ADMIN	-p
PASSWD2	User's extended password used for establishing connection#2	1-40 single-byte characters#3	ADMIN	-p2
LANG	User language used for connection	Japanese and English are supported. 2-byte ISO ID or 1-byte language key that is used in the SAP system: • Japanese: JA or J • English: EN or E	None	-l
CODEPAGE	Code page used to convert character codes in the Unicode version of the SAP system at the destination	Value combined with the language in the LANG label#4	None	-codepage

#1

The user specified in this label must have already been granted the following authorizations:

Table 2–99: Authorizations required by the user to establish RFC connection with function modules (S_RFC)

Authorization	Description	Value
RFC_TYPE	Type of RFC object to be protected	FUGR (function group)
RFC_NAME	RFC name to be protected	*

Authorization	Description	Value
ACTVT	Activity	16 (execution)

Table 2–100: Authorizations required for use of external management interfaces (S_XMI_PROD)

Authorization	Description	Value
EXTCOMPANY	Company name of the external management tool	HITACHI
EXTPRODUCT	Program name of the external management tool	JP1
INTERFACE	Interface ID	XAL

You can use the following user types for the user specified in this label:

- Dialog
- System
- Communication
- Service

#2

Specify the PASSWD label if the SAP system is applying conventional password rules. Specify the PASSWD2 label if the SAP system is applying extended password rules. The PASSWD and PASSWD2 labels are mutually exclusive.

#3

A user's password or extended password that is used for establishing connection must consist of single-byte numeric characters (from 0 to 9), single-byte alphabetic characters (from a to z, A to Z), and the following single-byte symbols:

!, @, $, %, &, /, (,), =, ?, ', `, *, +, ~, #, -, _, ., :, {, [,], }, <, >, |

#4

Set the LANG and CODEPAGE labels in the applicable combination shown below. If any other combination of language and code page is specified, an encoding error might occur in the information acquired from the SAP system.

Table 2–101: Combination of language and code page specifications

Connection-target SAP system	Connection language	Language (LANG)	Code page (CODEPAGE)
Unicode version	Japanese	JA	8000
	English	EN	No need to specify. If you specify a code page, specify 1100.
Non-Unicode version	Japanese	JA	No need to specify. If you specify a code page, specify 8000.
	English	EN	No need to specify. If you specify a code page, specify 1100.

If you omit specification of the LANG label, the user language defined in the connection-target system is assumed.

If you omit specification of the CODEPAGE label, the default code page in the connection-target system is assumed.

COMMAND section

The COMMAND section specifies information about the work directory for the jr3slget command.

Table 2–102: Values permitted in the COMMAND section

Label	Description	Permitted values	Default value	Argument
WORKDIR	Work directory for the command	1 to 255 single-byte alphanumeric characters. If a relative path is specified, it is treated as the path relative to the current directory.	Current directory	N/A

TRACE section

The TRACE section specifies information about the message log and data log that store the history of system log information extraction.

Table 2–103: Values permitted in the TRACE section

Label	Description	Permitted values	Default value	Argument
MSGLOG_LEVEL	Message log collection level for saving application trace information: • 0: Do not collect • 1: Collect only errors • 2: Standard • 3: Details • 4: Debug	0-4	2	N/A
MSGLOG_SIZE	File size for collecting the message log: • 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF)) • 1-65535: Wraparound within the specified size (in kilobytes)	0-65535	512	N/A
MSGLOG_DIR	Message log file (jr3slget.log) collection-target directory	1-255 single-byte alphanumeric characters. The total length, including file name jr3slget.log, must not exceed 255 bytes. If a relative path is specified, it is treated as the path relative to the work directory for the command.	Work directory for the command (or the current directory if it has not been changed by the WORKDIR label in the COMMAND section)	N/A
DATALOG_LEVEL	Data log collection level for saving various types of data information for applications: • 0: Do not collect • 1: Collect only errors • 2: Standard • 3: Details • 4: Debug	0-4	2	N/A
DATALOG_SIZE	File size for collecting the data log: • 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF)) • 1-65535: Wraparound within the specified size (in kilobytes)	0-65535	512	N/A

Label	Description	Permitted values	Default value	Argument
DATALOG_DIR	Data log file (jr3slget.dat) collection-target directory	1-255 single-byte alphanumeric characters. The total length, including file name jr3slget.dat, must not exceed 255 bytes. If a relative path is specified, it is treated as the path relative to the work directory for the command.	Work directory for the command (or the current directory if it has not been changed by the WORKDIR label in the COMMAND section)	N/A

TARGET section

The TARGET section specifies information that identifies the system log information to be extracted.

Table 2–104: Values permitted in the TARGET section

Label	Description	Permitted values	Default value	Argument
SERVER	SAP instance name (the SAP instance name that has a dialog service, and which can be verified by transaction code SM51)	1 to 20 single-byte alphanumeric characters	None	-server

FORMAT section

The FORMAT section specifies the output format of the system log information.

Table 2–105: Values permitted in the FORMAT section

Label	Description	Permitted values	Default values	Argument
COLUMN	Output format of system log information	Field ID. For details about the field ID, see *jr3slget* command in *Chapter 1. Commands*.	Column 1: <TIME> Column 2: <INSTANCE> Column 3: <USER> Column 4: <PROGRAM> Column 5: <MSGNO> Column 6: <MSGTEXT>	N/A

EXTRACTFILE section

The EXTRACTFILE section specifies information about the output file for the system log information.

Table 2–106: Values permitted in the EXTRACTFILE section

Label	Description	Permitted values	Default value
TYPE	Format of file for storing system log information: • WRAP1 This file is in wraparound format, which means that data is overwritten when the amount of system log information reaches a specified value. • WRAP2 This format consists of the number of files specified in the NUM label. When the amount of data in the first file reaches a specified value, new data is written in the	WRAP1 or WRAP2	WRAP1

Label	Description	Permitted values	Default value
	second file from the top after all existing data is deleted from the second file. When all of the files are full, new data is again written in the first file, starting from the top after all existing data is deleted from the first file. If you configure a new environment for JP1/IM - Agent, we recommend that you specify WRAP2. If you want to change the format of storage files after you have started system operations, first stop any products monitoring the storage files, and then delete the storage files and their management files[#1].		
SIZE	Size of one storage file: - 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF)) - 1 to 65535: Wraparound within the specified size (kilobytes)	0 to 65535	10240
X2PATH	- WRAP1 specified in the TYPE label Specify the path to the storage file that is to be used when storage file output is specified in the -x2 option.[#1, #2] - WRAP2 specified in the TYPE label Specify the storage file that is to be used when storage file output is specified in the -x2 option.[#2, #3]	- WRAP1 specified in the TYPE label 1 through 251 bytes of single-byte alphanumeric characters[#4] - WRAP2 specified in the TYPE label 1 through 254 bytes of single-byte alphanumeric characters[#4]	--
NUM	Number of files to be written to when using the WRAP2 format. This field is applicable only when WRAP2 is specified in the TYPE label.	2 to 9	5

Legend:

--: Not applicable

#1

If the WRAP1 format is used, a management file having the name *storage-file-name*.ofs is created in the same directory as for the storage file.

Example:

If SYSLOG is specified as the storage file name, a management file named SYSLOG.ofs is created in addition to the SYSLOG file.

If you delete the storage file, you must also delete the management file.

#2

If you do not use the default storage location, the storage and management files will not be collected when you use the jpcras command. Therefore, in the event of a problem, you need to manually collect the storage and management files.

#3

A value in the range specified in the NUM label (default: 1 through 5) is assigned to this value to obtain the file name.

#4

If a relative path is specified, the command's working directory (directory specified in the WORKDIR label in the COMMAND section) is assumed as the current directory. If no working directory is specified, the directory listed below is assumed as the current directory.

Option section

The Option section specifies information that determines the base point for system log extraction.

You can set a time zone for the SAP system by editing the SAPTIMEZONEOFFSET setting in the Option section of the environment parameters file to which the system log information extraction function refers. By editing the SAPTIMEZONEOFFSET setting, you can correctly extract system log information even when the host on which JP1/IM - Agent is running and the SAP system use different time zones. If you do not set a label in this section, the default value is used.

For details about the recommended collection base time for remote monitoring, see *Notes on the collection base time*. For details about the precautions to be observed when setting a time zone for the SAP system, see *Notes on the SAP system time zone*.

Table 2–107: Values permitted in the Option section

Label	Description	Permitted value	Default value
SHIFTEXTRACTTIME#1	The collection base time (units: seconds) that determines the base point for extracting system log information. Relative to the time at which to perform the collection, specify a value that indicates the amount of time by which to shift the time period (defined by two time points) for which to extract system log information.	0-600	5
SAPTIMEZONEOFFSET#2	When the host on which JP1/IM - Agent is running and the SAP system use different time zones (including the case where one adopts daylight saving time while the other does not), set a time difference between the SAP system time zone and UTC (units: minutes).	-1440-+1440#3	Time zone of the host on which JP1/IM - Agent is running. For example, when JP1/IM - Agent uses JST (UTC+9) as the time zone, +540 is set.

#1

When you are to specify 0 or a greater value, you can omit the plus sign (+).

#2

If, due to the processing delay in the SAP system, the saved system log information does not correctly reflect the actual time at which it has arisen, set a value greater than the default value for this label.

#3

Set this label only when the host on which PFM - Agent is running and the one on which the monitored SAP system is running use different time zones in an environment where the remote monitoring function is used.

The following examples show how to set the collection base time and the time zone:

- When 10 seconds is to be set as the collection base time

```
[Option]
SHIFTEXTRACTTIME=10
```

- When UTC (UTC+0) is set as the SAP system time zone and standard time is used

```
[Option]
SAPTIMEZONEOFFSET=0
```

- When EST (UTC-5) is set as the SAP system time zone and daylight saving time (+1 hour) is used

```
[Option]
SAPTIMEZONEOFFSET=-240
```

Notes

If you change the time zone set for the SAP system (except when such a change is necessitated by the switch between standard time and daylight saving time), you have to delete the file storing the time stamps that are based on the previously set time zone. If the timestamp file specified for the `-lasttime` option of the `jr3slget` command exists, delete it before resuming command execution.

Notes on the collection base time

Observe the following precautions when setting the collection base time:

- Add the `Option` section and the `SHIFTEXTRACTTIME` label when you create or update the environment parameters file.
- Make adjustments to the collection base time recommended for remote monitoring by taking into account the following concept behind the recommended collection base time:

  Concept behind the collection base time

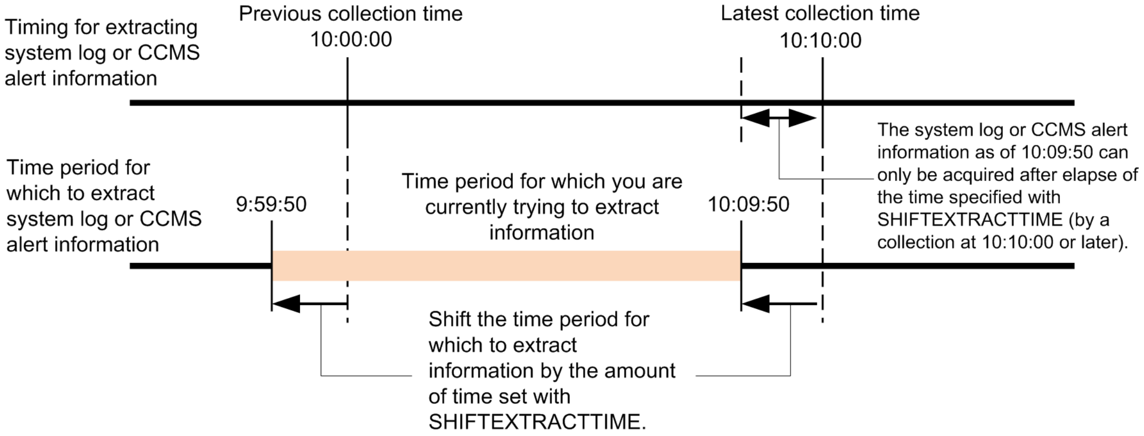
  Due to processing delay in the SAP system, the saved system log or CCMS alert information may not accurately reflect the actual time at which it arose. In this case, even when the local host is being monitored, some of the system log or CCMS alert information is not extracted, which is the same as what happens when a time delay in the SAP system (time difference between hosts) exceeds the collection base time. To avoid this problem, the default collection base time is set at 5 seconds. When a remote host is to be monitored, the effect of time delay in the SAP system must also be taken into consideration, and therefore 5 more seconds (which gives sufficient margin to accommodate an environment that meets the prerequisite of keeping a time difference between hosts to less than 1 second) is added to the collection base time, with 10 seconds being set as the recommended collection base time.

Notes on the SAP system time zone

Observe the following precautions when setting a time zone for the SAP system:

- The sample file for the environment parameters file does not contain the `Option` section or the `SAPTIMEZONEOFFSET` label. You have to add them when you create an environment parameters file.
- The system log or CCMS alert information that has arisen in the SAP system can be viewed from the JP1 side only after it is collected after elapse of the time set with `SHIFTEXTRACTTIME`. When changing the recommended `SHIFTEXTRACTTIME` setting, you have to take into account a delay in the collection timing. The following figure shows how the `SHIFTEXTRACTTIME` setting affects the extraction of system log or CCMS alert information.

Figure 2–12: How the SHIFTEXTRACTTIME setting affects the range of information to be extracted


Timing for extracting system log or CCMS alert information
Previous collection time 10:00:00
Latest collection time 10:10:00
Time period for which to extract system log or CCMS alert information
9:59:50
Time period for which you are currently trying to extract information
10:09:50
The system log or CCMS alert information as of 10:09:50 can only be acquired after elapse of the time specified with SHIFTEXTRACTTIME (by a collection at 10:10:00 or later).
Shift the time period for which to extract information by the amount of time set with SHIFTEXTRACTTIME.

Sample file of environment parameters file for jr3slget command (jr3slget.ini.sample)

Format

```
[CONNECT]
ASHOST=localhost
SYSNR=00
CLIENT=000
USER=CPIC
PASSWD=ADMIN
;PASSWD2=ADMIN
;LANG=JA
;CODEPAGE=8000

[COMMAND]
WORKDIR=../data/sap/command/jr3slget

[TRACE]
MSGLOG_LEVEL=2
MSGLOG_SIZE=512
MSGLOG_DIR=.
DATALOG_LEVEL=2
DATALOG_SIZE=512
DATALOG_DIR=.

[TARGET]
;SERVER=

[FORMAT]
;COLUMN=<TIME>
;COLUMN=<INSTANCE>
;COLUMN=<USER>
;COLUMN=<PROGRAM>
;COLUMN=<MSGNO>
;COLUMN=<MSGTEXT>

[EXTRACTFILE]
TYPE=WRAP2
NUM=5
SIZE=10240
X2PATH=SYSLOG
```

File

jr3slget.ini.sample

Storage directory

- Integrated agent host

In Windows:

- For a physical host

Folder-to-extract-the-archive-file#-for-SAP-system-monitoring-for-Windows`\sap_windows\command\agtm\evtrap\`

#

Agent-path`\options\sap_windows_`**VVRRSS**`.zip`

In Linux:

- For a physical host

Directory-to-extract-the-archive-file#-for-SAP-system-monitoring-for-Linux`/sap_linux/command/agtm/evtrap/`

#

`/opt/jp1ima/options/sap_linux_`**VVRRSS**`.tar.gz`

Description

This is the input file of the jr3slget command used for SAP system monitoring. Since various environmental parameters are predefined, they must be created by the user. The user copies the sample file (jr3slget.ini.sample) and changes the file name of the destination to "*any name*.ini" and uses it.

For details on where to locate the files, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Note that the location of the default environment parameters file (the file that the system searches when -cnf option is not specified) is .ini of the command in the current directory when the command is executed.

Character code

ASCII

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

When the command is executed using Script exporter, it is reflected when Script exporter is restarted. If you execute the command in any other way, it will be reflected when you save the file.

Information that is specified

See *Environment parameters file for jr3slget command (jr3slget.ini)*.

- `COMMAND` section

- WORKDIR label

  The WORKDIR label is set to change the working directory of the command from the default. The user must have created a directory with the path set in the WORKDIR label.

  If multiple environment parameters files are created, such as when monitoring a multi-instance SAP system using the SAP system log extract command, a different path must be set for each WORKDIR label.

  When Script exporter is used to execute the SAP system log extract command and the following values are set, a log file for the SAP system log extract command, a trace file for the SAP system log extract command, and a trace file for RFC library are output to the directory below, with the path relative to the working directory specified in service definition file of Script exporter.

```
../data/sap/command/jr3slget
```

- EXTRACTFILE section

- TYPE label

  If you use the script execution result monitoring function (Fluentd) to monitor output text files, you must specify the output format in WRAP2. When monitoring using the script execution result monitoring function (JP1/Base), it is also recommended to specify WRAP2.

Environment parameters file for jr3alget command (jr3alget.ini)

If you specify an environment parameters file as an argument in the `jr3alget` command, the command extracts the CCMS alert information of the SAP system based on the settings in the file.

You create this environment parameters file as a text file.

Setup procedure

To set up the environment parameters file:

1. Before you edit the environment parameters file, check that the `jr3alget` command is not running.

2. To create a new environment parameters file, copy the sample environment parameters file under the name `jr3alget.ini`.

   This `jr3alget.ini` becomes the default environment parameters file. The sample file of environment parameters file is as follows:

   ■Integrated agent host

   In Windows:

   - For a physical host:

     Folder-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Windows*`\sap_windows\command\agtm\evtrap\jr3alget.ini.sample`

     #: *Agent-path*`\options\sap_windows_`*VVRRSS*`.zip`

   In Linux:

   - For a physical host:

     Directory-to-extract-the-archive-file#*-for-SAP-system-monitoring-for-Linux*`/sap_linux/command/agtm/evtrap/jr3alget.ini.sample`

     #: `/opt/jp1ima/options/sap_linux_`*VVRRSS*`.tar.gz`

3. Open the `jr3alget.ini` file.

4. Edit the settings.

   The settings in the default environment parameters file are as follows; for details about the settings, see *Settings*:

   zum06005.tif

   In the case of an item that begins with a semicolon (`;`), the setting is disabled by default, because the semicolon indicates that it is a comment line. To enable the setting, remove the semicolon.

5. Save the environment parameters file.

   By specifying the `-cnf` option in the `jr3alget` command, you can extract the CCMS alert information of the SAP system based on the settings in the environment parameters file.

Settings

Specify the settings in the environment parameters file in the following format:

```
[section]
label=value
label=value
...
...
```

```
[section]
label=value
label=value
```

Notes

- Do not specify any unneeded characters, such as spaces at the beginning of a line or before and after an equals sign (=).
- The values specified in *section* and *label* are not case-sensitive.
- A line beginning with a semicolon (;) is treated as a comment.

The following tables describe the contents of each section in the environment parameters file. In a table, the *Argument* column indicates the argument that is specified in the `jr3alget` command, if applicable. N/A means that the item cannot be specified with the command.

CONNECT section

The `CONNECT` section specifies information needed to establish RFC connection with the SAP system at the time of command execution.

Table 2–108: Values permitted in the CONNECT section

Label	Description	Permitted values	Default value	Argument
`ASHOST`	Host name of the connection-target application server (which can be verified by transaction code `SM51`)	1 to 100 single-byte alphanumeric characters in one of the following formats: • Host name specified in the `hosts` file • IP address • SAP router address	`localhost`	`-h`
`SYSNR`	System number that can be identified by the connection-target application server host	0-99	`00`	`-s`
`CLIENT`	User's client name used for establishing connection	0-999	`000`	`-c`
`USER`	User name used for establishing connection[#1]	1 to 12 single-byte alphanumeric characters	`CPIC`	`-u`
`PASSWD`	User's password used for establishing connection[#2]	1 to 8 single-byte characters[#3]	`ADMIN`	`-p`
`PASSWD2`	User's extended password used for establishing connection[#2]	1 to 40 single-byte characters[#3]	`ADMIN`	`-p2`
`LANG`	User language used for connection	Japanese and English are supported. 2-byte ISO ID or 1-byte language key that is used in the SAP system: • Japanese: `JA` or `J` • English: `EN` or `E`	None	`-l`
`CODEPAGE`	Code page used to convert character codes in the Unicode version of the SAP system at the destination	Value combined with the language in the `LANG` label[#4]	None	`-codepage`

#1

The user specified in this label must have already been granted the following authorizations:

Table 2–109: Authorizations required by the user to establish RFC connection with function modules (S_RFC)

Authorization	Description	Value
RFC_TYPE	Type of RFC object to be protected	FUGR (function group)
RFC_NAME	RFC name to be protected	*
ACTVT	Activity	16 (execution)

Table 2–110: Authorizations required for use of external management interfaces (S_XMI_PROD)

Authorization	Description	Value
EXTCOMPANY	Company name of the external management tool	HITACHI
EXTPRODUCT	Program name of the external management tool	JP1
INTERFACE	Interface ID	XAL

You can use the following user types for the user specified in this label:

- Dialog
- System
- Communication
- Service

#2

Specify the PASSWD label if the SAP system is applying conventional password rules. Specify the PASSWD2 label if the SAP system is applying extended password rules. The PASSWD and PASSWD2 labels are mutually exclusive.

#3

A user's password or extended password that is used for establishing connection must consist of single-byte numeric characters (from 0 to 9), single-byte alphabetic characters (from a to z, A to Z), and the following single-byte symbols:

!, @, $, %, &, /, (,), =, ?, ', `, *, +, ~, #, -, _, ., :, {, [,], }, <, >, |

#4

Set the LANG and CODEPAGE labels in the applicable combination shown below. If any other combination of language and code page is specified, an encoding error might occur in the information acquired from the SAP system.

Table 2–111: Combination of language and code page specifications

Connection-target SAP system	Connection language	Language (LANG)	Code page (CODEPAGE)
Unicode version	Japanese	JA	8000
	English	EN	No need to specify. If you specify a code page, specify 1100.
Non-Unicode version	Japanese	JA	No need to specify. If you specify a code page, specify 8000.
	English	EN	No need to specify. If you specify a code page, specify 1100.

If you omit specification of the LANG label, the user language defined in the connection-target system is assumed.

If you omit specification of the CODEPAGE label, the default code page in the connection-target system is assumed.

COMMAND section

The COMMAND section specifies information about the work directory for the jr3alget command.

Table 2–112: Values permitted in the COMMAND section

Label	Description	Permitted values	Default value	Argument
WORKDIR	Work directory for the command	1 to 255 single-byte alphanumeric characters. If a relative path is specified, it is treated as the path relative to the current directory.	Current directory	N/A

TRACE section

The TRACE section specifies information about the message log and data log that store the history of CCMS alert information extraction.

Table 2–113: Values permitted in the TRACE section

Label	Description	Permitted values	Default value	Argument
MSGLOG_LEVEL	Message log collection level for saving application trace information: • 0: Do not collect • 1: Collect only errors • 2: Standard • 3: Details • 4: Debug	0-4	2	N/A
MSGLOG_SIZE	File size for collecting the message log: • 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF)) • 1-65535: Wraparound within the specified size (in kilobytes)	0-65535	512	N/A
MSGLOG_DIR	Message log file (jr3alget.log) collection-target directory	1 to 255 single-byte alphanumeric characters. The total length, including file name jr3alget.log, must not exceed 255 bytes. If a relative path is specified, it is treated as the path relative to the work directory for the command.	Work directory for the command (or the current directory if it has not been changed by the WORKDIR label in the COMMAND section)	N/A
DATALOG_LEVEL	Data log collection level for saving various types of data information for applications: • 0: Do not collect • 1: Collect only errors • 2: Standard • 3: Details • 4: Debug	0-4	2	N/A
DATALOG_SIZE	File size for collecting data log: • 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF))	0-65535	512	N/A

Label	Description	Permitted values	Default value	Argument
	- 1-65535: Wraparound within the specified size (in kilobytes)			
DATALOG_DIR	Data log file (jr3alget.dat) collection-target directory	1 to 255 single-byte alphanumeric characters. The total length, including file name jr3alget.log, must not exceed 255 bytes. If a relative path is specified, it is treated as the path relative to the work directory for the command.	Work directory for the command (or the current directory if it has not been changed by the WORKDIR label in the COMMAND section)	N/A

TARGET section

The TARGET section specifies information that identifies the CCMS alert information to be extracted.

Table 2–114: Values permitted in the TARGET section

Label	Description	Permitted values	Default values	Argument
MONITOR_SET	Monitor set name (for details, see the -ms option)	1 to 60 single-byte alphanumeric characters	SAP CCMS Technical Expert Monitors	-ms
MONITOR	Monitor name (for details, see the -mn option)	1 to 60 single-byte alphanumeric characters	All Monitoring Contexts	-mn

FORMAT section

The FORMAT section specifies the output format of the CCMS alert information.

Table 2–115: Values permitted in the FORMAT section

Label	Description	Permitted values	Default values	Argument
COLUMN	Output format of CCMS alert information	Field ID. For details about the field ID, see *Output format and contents* of *jr3alget* in *Chapter 1 Commands*.	Column 1: <ALERTDATE> Column 2: <ALERTTIME> Column 3: <MTSYSID> Column 4: <MTMCNAME> Column 5: <OBJECTNAME> Column 6: <FIELDNAME> Column 7: <VALUE> Column 8: <SEVERITY> Column 9: <MSG>	N/A
TIMEZONE	Time zone for time information specified in field IDs <ALERTDATE>, <ALERTTIME>, <STATCHGDAT>, and <STATCHGTIM>	- UTC Output in UTC (international time standard). - LOCAL Output in the local time at the location of the user who executed the command.	UTC	TIMEZONE

EXTRACTFILE section

The EXTRACTFILE section specifies information about the output file for the CCMS alert information.

Table 2–116: Values permitted in the EXTRACTFILE section

Label	Description	Permitted values	Default value
TYPE	Format of file for storing CCMS Alert Information: - WRAP1 This file is in wraparound format, which means that data is overwritten when the amount of CCMS Alert Information reaches a specified value. - WRAP2 This format consists of the number of files specified in the NUM label. When the amount of data in the first file reaches a specified value, new data is written in the second file, starting at the top, after all existing data is deleted from the second file. When all of the files are full, new data is again written in the first file, starting at the top, after all existing data is deleted from the first file. If you configure a new environment for JP1/IM - Agent, we recommend that you specify WRAP2. If you want to change the format of storage files after you have started system operations, first stop any products monitoring the storage files, and then delete the storage files and their management files#1.	WRAP1 or WRAP2	WRAP1
SIZE	Size of one storage file: - 0: 2 GB (the maximum value that can be expressed by a 32-bit signed integer (0x7FFFFFFF)) - 1 to 65535: Wraparound within the specified size (kilobytes)	0 to 65535	10240
X2PATH	- WRAP1 specified in the TYPE label Specify the path of storage file that is to be used when storage file output is specified in the -x2 option.#1, #2 - WRAP2 specified in the TYPE label Specify the storage file that is to be used when storage file output is specified in the -x2 option.#3, #4	- WRAP1 specified in the TYPE label 1 through 251 bytes of single-byte alphanumeric characters#4 - WRAP2 specified in the TYPE label 1 through 254 bytes of single-byte alphanumeric characters#4	--
NUM	Number of files to be stored in the WRAP2 format. This is applicable only when WRAP2 is specified in the TYPE label.	2 to 9	5

Legend:

--: Not applicable

#1

If the WRAP1 format is used, a management file having the name *storage-file-name*.ofs is created in the same directory as for the storage file.

Example:

If ALERT is specified as the storage file name, a management file named ALERT.ofs is created in addition to the ALERT file.

If you delete the storage file, you must also delete the management file.

#2

If you do not use the default storage location, the storage and management files will not be collected when using the jpcras command. Therefore, in the event of a problem, you need to manually collect the storage and management files.

#3

A value in the range specified in the NUM label (default: 1 through 5) is assigned to this value to obtain the file name.

#4

If a relative path is specified, the command's working directory (directory specified in the WORKDIR label in the COMMAND section) is assumed as the current directory. If no working directory is specified, the directory listed below is assumed as the current directory.

Option section

The Option section specifies information that determines the base point for extracting CCMS alert information. If you do not set a label in this section, the default value is used.

For details about the recommended collection base time for remote monitoring, see *Notes on the collection base time*.

Table 2–117: Values permitted in the Option section

Label	Description	Permitted value	Default value
SHIFTEXTRACTTIME#	The collection base time (units: seconds) that determines the base point for extracting CCMS alert information. Relative to the time at which to perform the collection, specify a value that indicates the amount of time by which to shift the time period (defined by two time points) for which to extract CCMS alert information.	0-600	5

#

If, due to the processing delay in the SAP system, the saved CCMS alert information does not correctly reflect the actual time at which it has arisen, set a value greater than the default value for this label.

The following example shows how to set the collection base time:

- When 10 seconds is to be set as the collection base time

```
[Option]
SHIFTEXTRACTTIME=10
```

Notes on the collection base time

Observe the following precautions when setting the collection base time:

- Add the Option section and the SHIFTEXTRACTTIME label when you create or update the environment parameters file.
- Make adjustments to the collection base time recommended for remote monitoring by taking into account the following concept behind the recommended collection base time:

  Concept behind the collection base time

  Due to processing delay in the SAP system, the saved system log or CCMS alert information may not accurately reflect the actual time at which it arose. In this case, even when the local host is being monitored, some of the system log or CCMS alert information is not extracted, which is the same as what happens when a time delay in the SAP system (time difference between hosts) exceeds the collection base time. To avoid this problem, the default collection base time is set at 5 seconds. When a remote host is to be monitored, the effect of time delay in the SAP system must also be taken into consideration, and therefore 5 more seconds (which gives sufficient margin to accommodate an environment that meets the prerequisite of keeping a time difference between hosts to less than 1 second) is added to the collection base time, with 10 seconds being set as the recommended collection base time.

Sample file of environment parameters file for jr3alget command (jr3alget.ini.sample)

Format

```
[CONNECT]
ASHOST=localhost
SYSNR=00
CLIENT=000
USER=CPIC
PASSWD=ADMIN
;PASSWD2=ADMIN
;LANG=JA
;CODEPAGE=8000

[COMMAND]
WORKDIR=../data/sap/command/jr3alget

[TRACE]
MSGLOG_LEVEL=2
MSGLOG_SIZE=512
MSGLOG_DIR=.
DATALOG_LEVEL=2
DATALOG_SIZE=512
DATALOG_DIR=.

[TARGET]
;MONITOR_SET=SAP CCMS Technical Expert Monitors
;MONITOR=All Monitoring Contexts

[FORMAT]
;COLUMN=<ALERTDATE>
;COLUMN=<ALERTTIME>
;COLUMN=<MTSYSID>
;COLUMN=<MTMCNAME>
;COLUMN=<OBJECTNAME>
;COLUMN=<FIELDNAME>
;COLUMN=<VALUE>
;COLUMN=<SEVERITY>
;COLUMN=<MSG>

[EXTRACTFILE]
TYPE=WRAP2
NUM=5
SIZE=10240
X2PATH=ALERT
```

File

jr3alget.ini.sample

Storage directory

- Integrated agent host

In Windows:

- For a physical host

Folder-to-extract-the-archive-file#-for-SAP-system-monitoring-for-Windows`\sap_windows\command\agtm\evtrap\`

#

Agent-path`\options\sap_windows_`**VVRRSS**`.zip`

In Linux:

- For a physical host

Directory-to-extract-the-archive-file#-for-SAP-system-monitoring-for-Linux`/sap_linux/command/agtm/evtrap/`

#

`/opt/jp1ima/options/sap_linux_`**VVRRSS**`.tar.gz`

Description

This is the input file of the jr3alget command used for SAP system monitoring. Since various environmental parameters are predefined, they must be created by the user. The user copies the sample file (jr3alget.ini.sample) and changes the file name of the destination to "*any name*.ini" and uses it.

For details on where to locate the files, see *Appendix A.4(3) Integrated agent host (Windows)* and *Appendix A.4(4) Integrated agent host (Linux)* in the JP1/Integrated Management 3 - Manager Overview and System Design Guide.

Note that the location of the default environment parameters file (the file that the system searches when -cnf option is not specified) is .ini of the command in the current directory when the command is executed.

Character code

ASCII

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

If the command is executed using the script exporter, it will be reflected when the script exporter is restarted. If the command is executed by any other method, it will be reflected when the file is saved.

Information that is specified

See *Environment parameters file for jr3alget command (jr3alget.ini)*.

- COMMAND section

- WORKDIR label

  The WORKDIR label is set to change the working directory of the command from the default. The user must have created a directory with the path set in the WORKDIR label.

  If multiple environment parameters files are created, such as when monitoring a multi-instance SAP system using the SAP system log extract command, a different path must be set for each WORKDIR label.

When Script exporter is used to execute the SAP system log extract command and the following values are set, a log file for the SAP system log extract command, a trace file for the SAP system log extract command, and a trace file for RFC library are output to the directory below, with the path relative to the working directory specified in service definition file of Script exporter.

```
../data/sap/command/jr3alget
```

- EXTRACTFILE section

- TYPE label

  If you use the script execution result monitoring function (Fluentd) to monitor output text files, you must specify the output format in WRAP2. When monitoring using the script execution result monitoring function (JP1/Base), it is also recommended to specify WRAP2.

Log metrics definition file (fluentd_*any-name*_logmetrics.conf)

Syntax

```
## Input
<worker worker-ids-used-for-the-log-metrics-feature>
  <source>
    @type prometheus
    bind bind-number
    port listening-port-number
    metrics_path metrics-path
  </source>
</worker>

<worker worker-id>
  <source>
    @type tail
    path absolute-path-of-the-log-file-monitored-by-the-log-metrics-feature
    tag user-specified-tag-value
    pos_file ../data/fluentd/tail/user-specified-tag-value.pos
[
    <parse>
      @type regular-expression-type
      expression regular-expressions-for-log-messages
      time_key time-variable-specified-in-expression
      time_format time_key-format
      types variable-name-specified-in-expression:type
    </parse>
]
  </source>

## Output
  <match tag-to-which-this-match-applies>
    @type prometheus
    <metric>
      name user-specified-log-metric-name
      type log-metric-type
      desc log-metric-description
      key key-for-determining-which-logs-are-converted-to-log-metrics
      buckets histogram-bucket
      <labels>
      label-key label-value
      </labels>
    </metric>
  </match>
</worker>
```

File

`fluentd_`*any-name*`_logmetrics.conf`

An *any-name* can contain half-width alphanumeric characters, hyphens, and underscores. The number of characters that can be specified is from 1 to 30.

Storage directory

For Windows

When using a physical host

Agent-path`\jp1ima\conf\user\`

When using a logical host

shared-folder`\jp1ima\conf\user\`

For Linux

When using a physical host

`/opt/jp1ima/conf/user/`

When using a logical host

shared-directory`/jp1ima/conf/user/`

Description

The Fluentd metric definition file used to read logs output by the application being monitored and convert them into log metrics. Create and place this file to use the log metrics feature.

In addition, in order to read this file, add an include setting to the log monitoring target definition file (jpc_fluentd_common_list.conf), and specify the name of this file.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows; CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in Fluentd behavior when restarting the Fluentd service.

Content description

- Input plug-in feature definitions

For details on the input plug-in feature, see *3.15.2(1) Input plug-in capability* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

- Setup used for Prometheus scraping

Configure settings using the first `<source>` of the `## Input` shown in *Syntax*.

Specify `prometheus` in `@type`.

bind-number (optional)

This specifies the binding interface when Prometheus scrapes metrics for this plug-in. If this item does not exist, the value is set to `0.0.0.0` by default.

listening-port-number (required)

Specify the listening port number `24820` used when Prometheus scrapes metrics for this plug-in. To change the listening port number, specify a different value.

metrics-path (optional)

This specifies the HTTP endpoint used when Prometheus scrapes metrics for this plug-in. If this item does not exist, the value is set to `/metrics` by default.

The number of characters that can be specified is from 1 to 255 (not including the / at the beginning).

worker-ids-used-for-the-log-metrics-feature (required)

Specify the worker ID of the worker used in "*Setup for a log file to be monitored by the log metrics feature*". To specify a single worker, use `<worker` *worker-id*`>`; to specify a range of multiple workers, use `<worker` *worker-id (minimum value)* `-` *worker-id (maximum value)*`>`.

- Setup for a log file to be monitored by the log metrics feature

Configure settings using the second `<source>` of the `## Input` shown in *Syntax*.

For the first `@type`, specify `tail`. For the `@type` under `<parse>`, specify the *supported range of the log monitoring feature* (either `regexp`, `syslog`, `csv`, `tsv`, `ltsv`, `multiline`, or `none`).

For details on the `tail` and `<parse>` setup, see *3.15.3(2) input plug-in feature* (Input Plugins) for the *3.15.3 log monitoring feature by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

user-specified-tag-value (required)

Specify character strings separated by a dot (`.`). (Example: `myapp.access`)

Character strings can contain lower-case alphabetical characters, numeric characters, and underscores. The number of characters that can be specified is from 1 to 30.

regular-expression-type (required)

This specifies the format of log files targeted by the log metrics feature when read into Fluentd. The following shows the types that can be specified:

- regexp
- syslog
- csv
- tsv
- ltsv
- multiline
- none

regular-expressions-for-log-messages (required or optional)

This setting is only written when the *regular-expression-type* is set to regexp. Specify the regular expression of the log message you want to read as the target of the log metrics feature here. Specifications of regular expressions follow Ruby regular expressions.

variable-name-specified-in-expression (optional)

This specifies the variable name used to specify the type of numerical value data extracted in *regular-expressions-for-log-messages*.

type (optional)

This specifies the type of the variable name specified in the *variable-name-specified-in-expression*. The following shows types that can be specified:

- integer
- float

worker-id (required)

Specify the worker ID to be used to monitor a log file in this `<source>` section from among ***worker-ids-used-for-the-log-metrics-feature*** specified in "*Setup used for Prometheus scraping*".

- Output plug-in feature definitions

For details on the output plug-in feature, see *3.15.2(2) Output plug-in capability* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Set these definitions using `## Output` shown in *Syntax*.

`<match` *tag-to-which-this-match-applies*`>` to `</match>` (optional)

In the match section, specify a tag to only apply `match` to Fluentd events assigned with the specified tag. If a tag is not specified, `match` is applied to all Fluentd events.

Specified values can contain half-width alphanumeric characters, hyphens, and underscores. The number of characters that can be specified is from 1 to 30.

`<metric>` to `</metric>`

Configure detailed log metrics settings in the metric section. Multiple metric sections can be defined for a single match section.

user-specified-log-metric-name (required)

This specifies the Prometheus metrics data name.

This must match the regular expression `[a-zA-Z_:][a-zA-Z0-9_:]*`. The number of characters that can be specified is from 1 to 255.

log-metric-type (required)

This specifies the metric type of the log metric in Prometheus (`counter` or `gauge`).

- `counter`

  This represents metrics that contain values that increase monotonically. This is suited to expressing the number of requests processed, completed tasks, and the number of errors, among other values.

  Cumulative values are only reset when restarting Fluentd.

  If the `key` in the definition is empty, the metrics value increases in increments of 1 for each record, regardless of record contents.

  For metrics that could have declining values, specify `gauge`.

- `gauge`

  This represents metrics that contain values that can increase or decrease. This is suited to expressing temperature values, current memory usage, and the number of simultaneous requests, among other values.

log-metric-description (required)

Enter the description of the log metric specified in the `description` of user-specific metric definitions.

Specified values can contain half-width alphanumeric characters, hyphens, and underscores. The number of characters that can be specified is from 1 to 255.

key-for-determining-which-logs-are-converted-to-log-metrics (required or optional)

This specifies the key for determining targets for conversion to log metrics. If the *log-metric-type* is counter, this is optional. If the *log-metric-type* is gauge, this is required.

The number of characters that can be specified is from 1 to 255.

label-key (optional)

A key can be specified for labels assigned to Prometheus metrics data.

This must match the regular expression `[a-zA-Z_:][a-zA-Z0-9_:]*`. This cannot begin with __. The number of characters that can be specified is from 1 to 255.

label-value (optional)

A value can be specified for the label key.

This can be specified using any Unicode characters other than control characters. The number of characters that can be specified is from 1 to 255.

When specifying a character string, the character string is set as the label value as is.

If either the *label-key* or the *label-value* is missing, the label will not be displayed.

The labels section, expressed using `<labels>` and `</labels>`, can be defined separately for both inside and outside the metric section. In addition, multiple labels (label sets including a *label-key* and a *label-value*) can be set. For details on labels, see *Label* and *A higher-level label section and the label section under the metric section* in *3.15.2(3)(b) prometheus output plug-in* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide 3.15.2 Log metrics by JP1/IM - Agent*.

Example of definitions

```
## Input
<source>
  @type prometheus
  bind '0.0.0.0'
  port 20723
  metrics_path /metrics
</source>

## Extract target log message 1
<source>
  @type tail
  @id logmetrics_counter
  path /usr/lib/WebAppA/ControllerLog/ControllerLog.log
  tag WebAppA.Controller
  pos_file /posfile/WebAppA/ControllerLog.log.pos
  <parse>
    @type regexp
    expression /^(?<logtime>[^\[]*) \[(?<loglebel>[^\]]*)\] (?<class>[^\[]*
) : endpoint "\/register" started. Target record: (?<record_num>\d[^\[]*).$/
    time_key logtime
    time_format %Y-%m-%d %H:%M:%S
    types record_num:integer
  </parse>
</source>

## Extract target log message 2
<source>
  @type tail
  @id logmeetrics_gauge
  path /usr/lib/WebAppA/GeneralLog/GeneralLog.log
  tag WebAppA.GeneralLog
  pos_file /posfile/WebAppA/GeneralLog.log.pos
  <parse>
    @type regexp
    expression /^(?<logtime>[^\[]*) \[(?<Status>[^\]]*)\] CPU Usage is (?<cp
uvalue>\d[^%]*)%.$/
    time_key logtime
    time_format %Y-%m-%d %H:%M:%S
    types cpuvalue:float
  </parse>
</source>
```

```
## Output
## Define log metrics 1 and 2
<match WebAppA.ControllerLog>
  @type prometheus
  <metric>
    name logmetrics_request_endpoint_register
    type counter
    desc The request number of endpoint register
  </metric>
  <metric>
    name logmetrics_num_of_registeredrecord
    type counter
    desc The number of registered record
    key record_num
    <labels>
    loggroup ${tag_parts[0]}
    log ${tag_parts[1]}
    </labels>
  </metric>
</match>

## Define log metric 3
<match WebAppA.GeneralLog>
  @type prometheus
  <metric>
    name logmetrics_cpu_usage
    type gauge
    desc the CPU Usage of WebAppA.
    key cpuvalue
    <labels>
    loggroup ${tag_parts[0]}
    log ${tag_parts[1]}
    </labels>
  </metric>
</match>
```

Property label definition file (property_labels.conf)

Syntax

```
{
  "character-string-before-replacement":"character-string-after-replacement
",
    ...
  },
}
```

File

`property_labels.conf`

Storage directory

For Windows

When using a physical host

Manager-path`\conf\imdd\plugin\jp1pccs_azure\`

When using a logical host

shared-folder`\jp1imm\conf\imdd\plugin\jp1pccs_azure\`

For Linux

When using a physical host

`/etc/opt/jp1imm/conf/imdd/plugin/jp1pccs_azure/`

When using a logical host

shared-directory`/jp1imm/conf/imdd/plugin/jp1pccs_azure/`

Description

The definition file used to convert IM management node property values into separate values. Set this to replace the tenant ID with the tenant name in Azure monitoring, for example. This also applies to extended attribute values for JP1 events. This file can be used to replace values in the setup description of each monitoring feature, provided that a corresponding value is available.

Character encoding

UTF-8 (without BOM)

Linefeed code

In Windows: CR+LF

In Linux: LF

Timing in which definitions are reflected

Definitions are reflected in the contents of the integrated operation viewer tree view when the jddcreatetree command and the jddupdatetree command are executed. Definitions are also reflected when a JP1 event is issued due to the monitoring of Promitor performance data triggering an alert.

Content description

character-string-before-replacement

Specify the property value you want to replace using 1 to 255 characters, excluding control characters.

Example of written description: Subscription ID

character-string-after-replacement

Specify the property value you want the *character-string-before-replacement* to be replaced with using 1 to 255 characters, excluding control characters.

Example of written description: Subscription name

imbase common configuration file (jpc_imbasecommon.json)

Format

```
{
    "tls_config": {
        "cert_file": "Server certificate File path",
        "key_file": "Server certificate key file path",
        "min_version": "Smallest TLS Protocol Version"
    }
    "http": {
        "max_content_length": Max Request Body Size,
        "client_timeout": Client Timeout
    }
}
```

File

`jpc_imbasecommon.json`

`jpc_imbasecommon.json.model` (model file)

Storage directory

■Integrated manager host

In Windows:

Manager-path`\conf\imdd\imagent\`

In Linux:

`/etc/opt/jp1imm/conf/imdd/imagent/`

Description

This configuration file defines Common operation of JP1/IM agent management base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflects when imbase and imbaseproxy services are Restart.

Information that is specified

Member name	Optional	Format	Value to Setup
tls_config	Yes	object	TLS Server Setup If this option is omitted, communication with the client is performed in plain text.

Member name		Optional	Format	Value to Setup
				The defaule value of member name is "`//tls_config`", treated as omitted. In order to enable TLS server setup, change it to "`tls_config`".
	cert_file	Not possible	string	Server Certificate File Path Specify the full path of the file under the following directory: • For Windows *Manager-path*`\conf\imdd\imagent\cert\` • For Liunx `/etc/opt/jp1imm/conf/imdd/imagent/cert/` For details, see the description of the files and directories that users can browse and edit on JP1/IM - Agent of the Integration Manager host agent on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	key_file	Not possible	string	Server certificate key file path Specify the full path of the file under the following directory: • For Windows *Manager-path*`\conf\imdd\imagent\secret\` • For Liunx `/etc/opt/jp1imm/conf/imdd/imagent/secret/` For details, see the description of the files and directories that users can browse and edit on JP1/IM - Agent of the Integration Manager host agent on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	min_version	Yes	string	The smallest TLS protocol Version to use during TLS negotiation (handshake) Specify one of the following: • TLSv1_2: TLS1.2 or higher • TLSv1_3: TLS1.3 If this operand is omitted or if an unspecified character string Value is specified, TLSv1_2 is assumed.
http		Yes	object	http Setup If it is omitted, the default Value is applied to the sub-items.
	max_content_length	Yes	number	Max size of REST API Request Body Specify within 1 to 10 (in MB). If this operand is omitted or if a numeric value that cannot be specified is specified, 10 is assumed.
	client_timeout	Yes	number	Time-out period for when a REST API is called Specify within the range of 1 to 600 (seconds). If this operand is omitted or if a value that cannot be specified is specified, 30 is assumed.

Notes

- If this File is not accessible under Physical host, the default Value is applied when all items are omitted.
- If this File cannot be accessed under Logical host, imbase and imbaseproxy will be stopped abnormally.
- If JSON format is invalid or specification does not match the type , imbase or imbaseproxy is stopped abnormally.

imbase configuration file (jpc_imbase.json)

Format

```
{
  "port": Listen port,
  "file_operation_timeout":"Timeout for File manipulation"
  "log": {
    "message": {
      "num": Logging sectors
      "size": Max. file size
    },
    "internal": {
      "level": "Logging Level"
      "num": Logging sectors
      "size": Max. file size
    },
    "access": {
      "num": Logging sectors
      "size": Max. file size
    }
  },
  "action": {
    "startup_action_check_timeout": Timeout period to transition actions tha
t remain in progress when the Unified Agent Management Platform is started t
o the terminal state
  }

}
```

File

`jpc_imbase.json`

`jpc_imbase.json.model` (model file)

Storage directory

■Integrated manager host

In Windows:

Manager-path`\conf\imdd\imagent\`

In Linux:

`/etc/opt/jp1imm/conf/imdd/imagent/`

Description

This configuration file defines the operation of imbase process in JP1/IM agent management base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

This information is reflected in imbase operation when imbase serviceis Restart.

Information that is specified

Member name			Optional	Format	Value to Setup
port			Yes	number	JP1/IM agent management base (imbase) listen port Specify within the range of 5001 to 65535. If this operand is omitted or if a numeric value that cannot be specified is specified, 20724 is assumed.
file_operation_timeout			Yes	number	If this time passes, File operator should abort the process Specify within the range of 1 to 60 (minutes). The default is 3. If omitted, or if an unspecified numeric value is specified, the default Value is assumed.
log			Yes	object	Logging Setup If it is omitted, the default Value is applied to the sub-items.
	message		Yes	object	Public log See *(a) Public log* in *12.2.1(6) Log of JP1/IM - Agent (JP1/IM Agent management base)* in the *JP1/Integrated Management 3 - Manager Administration Guide*. If it is omitted, the default Value is applied to the sub-items.
		num	Yes	number	Number of File sectors Specify within the range 2 to 99. If this operand is omitted or if a numeric value that cannot be specified is specified, 8 is assumed.
		size	Yes	number	Maximum file size Specify within 1 to 100 (in MB). If this operand is omitted or if a numeric value that cannot be specified is specified, 10 is assumed.
	internal		Yes	object	Internal log Logs that do not need to be referenced. If it is omitted, the default Value is applied to the sub-items.
		level	Yes	string	Log-level# Specify one of the following: • trace: debug logging and functional tracing • debug: info logging and debug logging • info: warn logging and informational logging • warn: error logging and Warning logging • error: Error Logging If this operand is omitted or if an unspecified character string Value is specified, info is assumed.
		num	Yes	number	Number of File sectors Specify within the range 2 to 99. If this operand is omitted or if a numeric value that cannot be specified is specified, 8 is assumed.
		size	Yes	number	Maximum file size Specify within 1 to 100 (in MB).

Member name	Optional	Format	Value to Setup
			If this operand is omitted or if a numeric value that cannot be specified is specified, 10 is assumed.
access	Yes	object	Access log Logs that do not need to be referenced. If it is omitted, the default Value is applied to the sub-items.
num	Yes	number	Number of File sectors Specify within the range 2 to 99. If this operand is omitted or if a numeric value that cannot be specified is specified, 8 is assumed.
size	Yes	number	Maximum file size Specify within 1 to 100 (in MB). If this operand is omitted or if a numeric value that cannot be specified is specified, 10 is assumed.
action	Yes	object	Configuring the Unified Agent Action Execution Feature If omitted, the default value is applied to the subitem.
startup_action_check_timeout	Yes	number	When the timeout period specified for this member elapses after starting the Unified Agent Management Platform, if the operation of the action cannot be confirmed for the action that remains running when the Unified Agent Management Platform is started, the action is moved to the end state. Specify in the range of 120 to 3600 (unit: seconds). The default is 120. If omitted or a numeric value that cannot be specified is specified, a default value is assumed.

Notes

- If this File is not accessible under Physical host, the default Value is applied when all items are omitted.
- If this File cannot be accessed under Logical host, imbase and imbaseproxy will be stopped abnormally.
- If JSON format is invalid or the type Does not match the type specified, imbase and imbaseproxy is stopped abnormally.

#:

The following shows the types of logs to be output depending on the log level.

Output log	Log level				
	trace	debug	info	warn	error
Function trace	Y	--	--	--	--
Debug information	Y	Y	--	--	--
Information	Y	Y	Y	--	--
Warning	Y	Y	Y	Y	--
Error	Y	Y	Y	Y	Y
Items that cannot be classified by the output Message of the deployment library, etc.	Y	Y	Y	Y	Y

Legend

Y: Output, --: Do not output

imbaseproxy configuration file (jpc_imbaseproxy.json)

Format

```
{
  "port": Listen port,
  "log": {
    "message": {
      "num": Logging sectors
      "size": Max. file size
    },
    "internal": {
      "level": "Logging Level"
      "num": Logging sectors
      "size": Max. file size
    },
    "access": {
      "num": Logging sectors
      "size": Max. file size
    }
  }
}
```

File

`jpc_imbaseproxy.json`

`jpc_imbaseproxy.json.model` (model file)

Storage directory

■Integrated manager host

In Windows:

Manager-path`\conf\imdd\imagent\`

In Linux:

`/etc/opt/jp1imm/conf/imdd/imagent/`

Description

This configuration file defines the operation of imbaseproxy process in JP1/IM agent management base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflected when imbaseproxy serviceis Restart.

Information that is specified

Member name	Optional	Format	Value to Setup
port	Yes	number	JP1/IM agent management base (imbaseproxy) listen port Specify within the range of 5001 to 65535. If this operand is omitted or if a numeric value that cannot be specified is specified, 20725 is assumed.
log	Yes	object	Logging Setup See *(a) Public log* in *12.2.1(6) Log of JP1/IM - Agent (JP1/IM Agent management base)* in the *JP1/Integrated Management 3 - Manager Administration Guide*. For information about Setup items, see log in imbase configuration file (jpc_imbase.json).

Notes

- If this File is not accessible under Physical host, the default Value is applied when all items are omitted.
- If this File cannot be accessed under Logical host, imbase or imbaseproxy will be stopped abnormally.
- If JSON format is invalid or does not match the type specified, imbase or imbaseproxy is stopped abnormally.

imagent common configuration file (jpc_imagentcommon.json)

Format

```
{
  "JP1_BIND_ADDR": Binding method,
  "COM_LISTEN_ALL_ADDR": Whether more than one IP address is listening for s
ervices,
  "COM_MAX_LISTEN_NUM": how many IP addresses that the service is listening
on,
  "JP1_CLIENT_BIND_ADDR": Binding method,
  "http": {
    "max_content_length": Max Request Body Size,
    "client_timeout": Client Timeout
  },
  "immgr": {
    "host": "Manager Host name",
    "proxy_url": "HTTP proxy server URL",
    "proxy_user": "HTTP Proxy Server authentication User name",
    "tls_config": {
      "ca_file": "CA Certificate File Path",
      "insecure_skip_verify": Server certificate validation skip,
      "min_version": "Smallest TLS Protocol Version"
    },
    "imbase": {
      "port": Connecting port of JP1/IM agent management base (imbase)
    },
    "imbaseproxy": {
      "port": Connecting port of  JP1/IM agent management base (imbaseproxy)
    }
  }
}
```

File

`jpc_imagentcommon.json`

`jpc_imagentcommon.json.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host

  Agent-path`\conf\`

- For a logical host

  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host

  `/opt/jp1ima/conf/`

- For a logical host

shared-directory`/jp1ima/conf/`

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This configuration file defines Common operation of JP1/IM agent control base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflects when imagent service or imagentaction service, or imagentproxy service restarts.

Information that is specified

Member name	Optional	Format	Value to Setup
JP1_BIND_ADDR	Yes	string	Server Binding Methods You can specify one of the following: • ANY: Do not bind (accepts all IP address) • IP: Binding to a IP address Retrieved by Host name Name Resolution It can be accepted for more than one IP address by specifying COM_LISTEN_ALL_ADDR and COM_MAX_LISTEN_NUM. If this operand is omitted or if an unspecified character string Value is specified, ANY is assumed.
COM_LISTEN_ALL_ADDR	Yes	number	Whether the service is listening on more than one IP address • 0:Bind with the highest-priority IP address • 1:Binding with more than one IP address If this operand is omitted, or if a numeric value that cannot be specified is specified, 0 is assumed.
COM_MAX_LISTEN_NUM	Yes	number	How many IP addresses on which the service is listening If you specify 1 for COM_LISTEN_ALL_ADDR, specify the number of IP address that the service listens on, ranging from 1 to 16.

Member name	Optional	Format	Value to Setup
			When this option is omitted or a value that cannot be specified is assumed to be 4.
JP1_CLIENT_BIND_ADDR	Yes	string	Source IP address Binding Method When Sending Requests You can specify one of the following: • ANY: Bind on all IP address • IP: Binding with IP address Retrieved from Host name Name Resolution If this operand is omitted or if an unspecified character string Value is specified, ANY is assumed.
http	Yes	object	See the explanation of http in imbase configuration file (jpc_imbase.json).
immgr	Not possible	object	Connect to JP1/IM Manager Host Setup
host	Not possible	string	Manager Host name
proxy_url	Yes	string	HTTP Proxy Server URL Use the following form. `http://`*Host-name-or-IPv4-address*`:`*Port-number(1024 to 65535)* If this operand is omitted or if a character string Value that cannot be specified is specified, HTTP proxy server is not used.
proxy_user	Yes	string	User name uses for HTTP authentication for HTTP proxies You can specify ASCII characters that do not contain control codes (except the Spacetab) and ":". Character types are not checked. If this option is omitted or if an unspecified character string Value is specified, authentication is not sent to HTTP proxy server.
tls_config	Yes	object	TLS Client Setup If this option is omitted, communication with imbase or imbaseproxy is not encrypted. The defaule value of member name is "`//tls_config`", treated as omitted. In order to enable TLS server setup, change it to "`tls_config`".
ca_file	Yes	string	CA certificate File of authentication authority that issued Server certificate for imbase or imbaseproxy Specifies CA certificate that is used to validate Server certificate. Specify the full path of the file under the following directory: ■In a non-cluster configuration • For Windows *Agent-path*`\conf\user\cert\` • For Linux `/opt/jp1ima/conf/user/cert/` ■In a cluster configuration • For Windows *shared-folder*`\jp1ima\conf\user\cert\` • For Linux *shared-directory*`/jp1ima/conf/user/cert/` For details, see the description of the files and directories that users can browse and edit on JP1/IM - Agent of the Integration Manager host agent on *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Member name			Optional	Format	Value to Setup
		insecure_skip_verify	Yes	boolean	If you do not want to validate Server certificate for imbase or imbaseproxy, specify true if you want to validate it false. By default, false is assumed.
		min_version	Yes	string	See the explanation of the min_version in imbase configuration file (jpc_imbase.json).
imbase			Not possible	object	Setup of the destination imbase
	port		Not possible	number	JP1/IM agent management base (imbase) listen port Specify within the range of 5001 to 65535. If this operand is omitted or if a numeric value that cannot be specified is specified, 20724 is assumed.
imbaseproxy			Not possible	object	Setup of the destination imbaseproxy
	port		Not possible	number	JP1/IM agent management base (imbaseproxy) listen port Specify within the range of 5001 to 65535. If this operand is omitted or if a numeric value that cannot be specified is specified, 20725 is assumed.

Notes

- If this File is not accessible, imagentproxy will be stopped abnormally.
- If JSON format is invalid or does not match the type specified, the service is stopped abnormally.

imagent configuration file (jpc_imagent.json)

Format

```
{
  "port": Listen port,
  "log": {
    "message": {
      "num": Logging sectors
      "size": Max. file size
    },
    "internal": {
      "level": "Logging Level"
      "num": Logging sectors
      "size": Max. file size
    },
    "access": {
      "num": Logging sectors
      "size": Max. file size
    }
  },
  "action": {
    "auto_action_concurrency": "Whether Response Action(auto) can execute si
multaneously",
    "max_concurrent_response_actions": max number of actions execute simulta
neously 1,
    "max_concurrent_file_operation_actions": max number of actions execute s
imultaneously 2,
    "auto_action_execution_result_limit": the limit of action result of comm
and execution 1,
    "manual_action_execution_result_limit": the limit of action result of co
mmand execution 2,
    "username": "user name",
    "domainname": "domain name",
    "shell": "shell command"
    "service_startup_wait_time": Service startup wait time

  }
}
```

File

`jpc_imagent.json`

`jpc_imagent.json.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host

  Agent-path`\conf\`

- For a logical host

  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This configuration file defines operation of imagent of JP1/IM agent control base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflects when imagent service and imagentaction service restarts.

Information that is specified

Member name		Optional	Format	Value to Setup
port		Yes	number	The port for accepting access to JP1/IM agent control base (imagent) Specify within the range of 5001 to 65535. The default is 20726.
log		Yes	object	Logging Setup See *(a) Public log* in *12.2.2(7) JP1/IM - Agent control base log* in the *JP1/Integrated Management 3 - Manager Administration Guide*. For details about setup items, see the description of `log` in the *imbase configuration file (jpc_imbase.json)*.
action		Yes	object	Setup of integrated agent Action Execute function If it is omitted, the default value is applied to the sub-items.
	auto_action_concurrency	Yes	string	Specifies whether to simultaneous execution of Action from auto Response Action of JP1/IM - Manager (defaults: no). You can specify one of the following: • `yes`: Concurrent Execute is enabled. • `no`: Concurrent Fail If this member is omitted, the default Value is assumed. For details, see *3.15.7(3)(a) Auto response Action* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	max_concurrent_response_actions	Yes	number	Specifies the max action concurrent execute count for action that was execute from auto responseAction or manual responseAction of JP1/IM - Manager, between `1` and `48` (default:`10`). If this member is omitted, the default Value is assumed. Error if the sum of the `max_concurrent_response_actions` and `max_concurrent_file_operation_actions` exceeds `48`.

Member name		Optional	Format	Value to Setup
				For details, see *3.15.7(3)(e) Maximum concurrent actions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	max_concurrent_file_operation_actions	Yes	number	Define JP1/IM - Manager Specifies the maximum concurrent execute of action that was execute from the definition file manipulation function, from `2` and `48` (default: `5`). If this member is omitted, the default value is assumed. Error if the sum of the `max_concurrent_deal_actions` and `max_concurrent_file_operation_actions` exceeds 48. For details, see *3.15.7(3)(e) Maximum concurrent actions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	auto_action_execution_result_limit	Yes	number	Specifies the upper limit of the lines of the command execute result (standard output or standard error output of the command) for commands execute from auto responseAction in JP1/IM - Manager, ranging from `0` to `196,600` lines (default: `1000` lines). If this member is omitted, the default Value is assumed. For details, see *3.15.7(1)(e) Command execution function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	manual_action_execution_result_limit	Yes	number	Specify the upper limit of the lines of command execute results (standard output or standard error output of commands) for commands execute from manual responseAction in JP1/IM - Manager in lines `0` to `196,600` (default: `1000` lines). If this member is omitted, the default Value is assumed. For details, see *3.15.7(1)(e) Command execution function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.
	username	Yes	string	The user that executes command; used for Action Execution Specify up to 20 bytes. If this option is omitted, works as "jp1imaction". You cannot specify a user name with multibyte characters. Specify the user that can log on and has a home directory. For Windows, there are the following precautions: • **Allow log on locally** security policy setting for the user is necessary. • The token of user is necessary to be able to be retrieved by Windows `LogonUser` function. • The password is necessary to be registered using the `jimasecret` command.
	domainname	Yes	string	The domain to which the user specified at username belongs It is available only in Windows. Specify up to 255 bytes. If this option is omitted, works as `"."`. You cannot specify a domain name with multibyte characters. When the user specified in `username` is local user, set `"."`.
	shell	Yes	string	The shell to execute command; used for Action Execution For Action Execution, the command specified with `-c` option is executed to the shell specified in this option. If this option is omitted, works in `"/bin/sh"`.
	service_startup_wait_time	Yes	number	Wait time for service startup in definition file update process.

Member name		Optional	Format	Value to Setup
				Specify the waiting time to confirm that the definition file reflection process has been performed correctly in the range of 5 to 120 (seconds). If omitted, it operates at 15 (seconds).

Notes

- If this file is not accessible, imagentproxy will be stopped abnormally.
- If JSON format is invalid or does not match the type specified, the service is stopped abnormally.

imagentproxy configuration file (jpc_imagentproxy.json)

Format

```
{
  "port": Listen port,
  "log": {
    "message": {
      "num": Logging sectors
      "size": Max. file size
    },
    "internal": {
      "level": "Logging Level"
      "num": Logging sectors
      "size": Max. file size
    },
    "access": {
      "num": Logging sectors
      "size": Max. file size
    }
  }
}
```

File

`jpc_imagentproxy.json`

`jpc_imagentproxy.json.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This configuration file defines the operation of imagentproxy of JP1/IM agent control base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflected when imagentproxy services Restart.

Information that is specified

Member name	Optional	Format	Value to Setup
port	Yes	number	The port for accepting access to JP1/IM agent control base (imagentproxy) Specify within the range of 5001 to 65535. The default is 20727.
log	Yes	object	Logging Setup See *(a) Public log* in *12.2.2(7) JP1/IM - Agent control base log* in the *JP1/Integrated Management 3 - Manager Administration Guide*. For details about setup items, see the description of `log` in the *imbase configuration file (jpc_imbase.json)*.

Notes

- If this file is not accessible, imagentproxy will be stopped abnormally.
- If JSON format is invalid or does not match the type specified, the service is stopped abnormally.

imagentaction configuration file (jpc_imagentaction.json)

Format

```
  "port": Listen port,
  "log": {
    "message": {
      "num": Logging sectors
      "size": Max. file size
    },
    "internal": {
      "level": "Logging Level"
      "num": Logging sectors
      "size": Max. file size
    },
    "access": {
      "num": Logging sectors
      "size": Max. file size
    }
  }
}
```

File

`jpc_imagentaction.json`

`jpc_imagentaction.json.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host
  shared-directory`/jp1ima/conf/`

Description

This configuration file defines the operation of imagentaction of JP1/IM agent control base.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Reflects when imagent service and imagentaction service Restart.

Information that is specified

Member name	Optional	Format	Value to Setup
port	Yes	number	The port for accepting access to JP1/IM agent control base (imagentaction) Specify within the range of 5001 to 65535. The default is 20728.
log	Yes	object	Logging Setup See *(a) Public log* in *12.2.2(7) JP1/IM - Agent control base log* in the *JP1/Integrated Management 3 - Manager Administration Guide*. For details about setup items, see the description of `log` in the *imbase configuration file (jpc_imbase.json)*.

Notes

- If this file is not accessible, imagentproxy will be stopped abnormally.
- If JSON format is invalid does not match the type specified, the service is stopped abnormally.

User-created definition file list definition file (jpc_user_deffile_list.json)

Format

- Format of definition File

```
{
  "filelist":[
    {
      "filename": "File Name",
      "filepath": "File's absolute path",
      "filecategoryID": "File Category ID",
      "filecategoryName": "File Category-name",
      "updateaction": "Manipulation for Defining Import"
    }, ...
  ]
}
```

- Model File format

```
{
  "filelist":[
    {
      "filename": "",
      "filepath": "",
      "filecategoryID": "",
      "filecategoryName": "",
      "updateaction": ""
    }
  ]
}
```

File

`jpc_user_deffile_list.json`

`jpc_user_deffile_list.json.model` (model file)

Storage directory

■Integrated agent host

In Windows:

- For a physical host
  Agent-path`\conf\`
- For a logical host
  shared-folder`\jp1ima\conf\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/`
- For a logical host

shared-directory/`jp1ima/conf/`

Description

user-created definition Files that can be updated and deleted with JP1/IM - Manager supplied REST API.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

The definition is read when the update function, delete function, or list acquisition function of the definition File is activated.

Information that is specified

Member name	Optional	Value to Setup
filename	Not possible	Indicates File.
filepath	Yes	Destination of File is written in absolute path. If File path (absolute path including File name) exceeds 200 characters, it becomes Error. If filepath does not contain "jp1ima\conf\user", it is considered an invalid File pass. If File with the name specified in filename does not exist in the specified Filepath It is regarded as an invalid definition. If this Setup option is omitted, the directory where JP1/IM - Agent is to be installed is assumed to be *Agent-path*/`conf/user` (for a logical environment, replace "*Agent-path*" with "*Shared-directory*/`jp1ima`).
filecategoryID	Yes	Describes the category ID to be specified when grouping more than one File. A File with the same category ID is considered to belong to the same category. Allowed characters are alphanumeric characters, "-" (hyphen), and "_" (underscore). Up to 32 characters can be specified. Category ID starting with "jp1_" cannot be specified.
filecategoryName	Yes	specifies the category name for category ID. Specify a character other than a control character. Up to 32 characters can be specified. If no filecategoryID is specified, this Setup field is ignored. If a filecategoryID is specified and this Setup field is not specified, filecategoryID's Value is Setup.
updateaction	Yes	For Windows, describe the action (command-line) to execute when the definition file is updated at the file destination directory that is the relative path from one layer upper from installed directory. For Linux, describe the action (command-line) to execute when the definition file is updated at the relative path from `/opt/`. For detail, see ■*Description of updateaction*.

■Description of updateaction

You can list the commands that is executed after updating File. The maximum length of a command line that can be written is 4096 bytes.

If Execute destination host is a 64-bit Windows and you specify commands that are located in the %WINDIR%\System32 folders or lower, be aware of WOW64 redirection feature.

The following types of commands can be Executed:

Hosts that Execute Commands Are Windows

- Execute Format File (.com,.exe)
- Batch File (.bat)
- The scripting File of JP1/Script (.spt) (but the association must be Setup so that .spt File can be Executed)

Hosts that Execute Commands Are Linux

- Linux Commands
- Shell scripts

Note that you cannot Execute the following commands:

- Commands that require interaction
- Command to display the screen
- Commands with escape sequences or control codes
- Commands that do not terminate, such as daemons
- Commands that require interaction with the desktop such as Windows Message mechanisms and DDE (for Windows)
- Commands that shutdown OS, such as shutdown and halt

■Definition File that can be specified for user-definition file list file

Definition File that can be specified	What to Execute if File is updated		Displayed category on GUI
	Command Execute	Command line	

Blackbox exporter Monitored (User-Defined) Discovery configuration file (file_sd_config_blackbox_ any name.yml)	Reload of Prometheus server	■In Windows
		• For a physical host
		`cmd.exe /c` *Agent-path*`\addon_management\prometheus\addon_jpc_service_reload.bat`
		• For a logical host
		`cmd.exe /c` *Agent-path*`\addon_management\prometheus\addon_jpc_service_reload.bat -h` *Logical-host*
		■In Linux
		• For a physical host
		`/bin/sh -c /opt/jp1ima/addon_management/prometheus/addon_jpc_service_reload`
		• For a logical host
		`/Bin/sh -c /opt/jp1ima/addon_management/prometheus/addon_jpc_service_reload -h` *Logical-host*
			jp1_imexporter

User-specific discovery configuration file (user_file_sd_config_ any name.yml)			

Definition File that can be specified	What to Execute if File is updated		Displayed category on GUI
	Command Execute	Command line	

Monitoring Fluentd's text-formatted log file definition file (fluentd_trap-name_tail.conf) #	Restart of Fluentd service	■In Windows
		• For a physical host
		`cmd.exe /c` *Agent-path*`\addon_management\fluentd\addon_jpc_service_reload.bat`
		• For a logical host
		`cmd.exe /c` *Agent-path*`\addon_management\fluentd\addon_jpc_service_reload.bat -h` *Logical-host*
		■In Linux
		• For a physical host
		`/bin/sh -c /opt/jp1ima/addon_management/fluentd/addon_jpc_service_reload`
		• For a logical host
		`/bin/sh -c /opt/jp1ima/addon_management/fluentd/addon_jpc_service_reload -h` *logical-host*
			jp1_imfluenntd

Monitoring Fluentd's Windows event-log definition file (fluentd_trap-name_wevt.conf) #			
CA Certificate File (for Blackbox exporter) #	Reload of Blackbox exporter	Same as Process exporter configuration file (jpc_blackbox_exporter.yml).	jp1_certificate
Client Certificate File (for Blackbox exporter) #			
Client Certificate Key File (for Blackbox exporter) #			
Password File (for Blackbox exporter)#			
Environment variable file (any File name) #	Not required (Environment variable file is referenced when the command Execution starts)	--	--

Log metrics definition file (fluentd_any name _logmetrics.conf)	Restart of Fluentd service	■In Windows
		• For a physical host
		`cmd.exe /c` *Agent-path*`\addon_management\fluentd\addon_jpc_service_reload.bat`
		• For a logical host
		`cmd.exe /c` *Agent-path*`\addon_management\fluentd\addon_jpc_service_reload.bat -h` *Logical-host*
		■In Linux
		• For a physical host
		`/bin/sh -c /opt/jp1ima/addon_management/fluentd/addon_jpc_service_reload`
		• For a logical host
			jp1_imfluentd

Definition File that can be specified	What to Execute if File is updated		Displayed category on GUI
	Command Execute	Command line	
		`/bin/sh -c /opt/jp1ima/addon_management/fluentd/addon_jpc_service_reload -h` *logical-host*	

Legend:

--: Not applicable

#

It can also be specified if File is Add or Deleted.

Definition file property file (jpc_file_properties.json)

Format

```
{
  "filelist":[
    {
      "filename": "File Name",
      "filepath": "File's absolute path",
      "updateaction": "Manipulation for Defining Import",
      "message": "Message"
    }, ...
  ]
}
```

File

`jpc_file_properties.json`

Storage directory

Place the definition File that you want to work with in the Get or Refresh functions of the definition File into the compressed zip File.

Description

This File describes File name, File path, and File import operations for the definition File that are to be manipulated by the acquisition or update functions of the definition File.

Character code

UTF-8 (without BOM)

Line feed code

In Windows: CR+LF

In Linux: LF

When the definitions are applied

Loads a definition when the retrieval or updating function of the definition File is activated.

Information that is specified

Item name	Description
filename	Indicates File.
filepath	Destination of File is written in absolute path. If File path (absolute path including File name) exceeds 200 characters, it becomes Error.
updateaction	Describes the action (command-line) that should be executed if File is updated. For detail, see ■*Description of updateaction* in *User-created definition file list definition file (jpc_user_deffile_list.json)*.
message	Returns the error message ID and its Message body. If it succeeds, omit this item.

Environment variable file (any file name)

Format

```
Environment variable name 1 = Variable Value 1
[Environment-variable-name-2 = Variable Value 2]
   :
```

File

File name is optional.

Storage directory

■Integrated agent host

In Windows:

Any integrated agent host folder# where you want to execute commands.

In Linux:

Any integrated agent host directory# where you want to execute commands.

#

The directory where Environment variable file is stored is arbitrary, but Environment variable file should not be stored in the directory for JP1/IM. If it is stored, it becomes the object of data collection and backup.

When File manipulation facility is used to operate Environment variable file, Environment variable file is stored in the following directory#:

In Windows:

- For a physical host
  Agent-path`\conf\user\`
- For a logical host
  shared-folder`\jp1ima\conf\user\`

In Linux:

- For a physical host
  `/opt/jp1ima/conf/user/`
- For a logical host
  shared-directory`/jp1ima/conf/user/`

#

When Environment variable file is operated by definition File manipulation function, Environment variable file is stored in the specified Storage directory. This directory is not subject to data collection or backup.

Description

A File that defines an environment-variable for Execute commands on JP1/IM managed hosts.

When you Execute a command on a JP1/IM managed host with auto Response Action, or manual Response Action in JP1/IM - Manager, you can specify an environment variable as execution environment for that command. Environment variables can be specified by Environment variable file written in the format described here.

You can specify any Environment variable for each command as making Environment variable files(File names are optional).

If Environment variable file is not specified in Windows environment, the command is executed in the system environment variable.

When the definitions are applied

Environment variable file is referenced when starting the command execution.

Character code

The encoding of Environment variable file is the character codes of the managed host that Execute the command. For the character codes, see the explanation of the character codes in *3.15.7(1)(e) Command execution function* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Line feed code

In Windows: CR+LF

In Linux: LF

Information that is specified

The maximum length of a character string that can be specified in a single line is 1023 bytes. Be sure to insert a line break at the end of each line.

Environment Variable Name

Specifies the name of the environment variable.

You cannot specify an environment variable that contains a newline character.

Value

Specifies Value of the environment-variable.

By specifying the system environment variable name here, Value of the system environment variable is inherited.

When specifying a system environment variable, enclose the system environment variable name in "<-" and "->", and then specify "<-variable->".

Important

- Do not specify a character string other than the format "environment variable name = variable Value". If this operand is specified, the command may terminate abnormally depending on the host-side OS that Execute the command.
- Note that Setup Value will not be encrypted or obfuscated if you include something like proxy Setup as an environment-variable.

About definition of common placeholders for descriptive items in yml file

The following is a general placeholder definition used in the description item of the .yml file.

Placeholder	Definition
<boolean>	Indicates a Boolean value that can have either "true" or "false" values.
<duration>	Indicates the duration that matches the following regular expressions: `((([0-9]+)y)?(([0-9]+)w)?(([0-9]+)d)?(([0-9]+)h)?(([0-9]+)m)?(([0-9]+)s)?(([0-9]+)ms)?|0)`
<filename>	Indicates a valid path in the current working directory.
<host>	Indicates a valid string consisting of a host name or internet address and an optional port number.
<int>	Indicates an integer value.
<labelname>	Indicates a string that matches the following regular expression: `[a-zA-Z_] [a-zA-Z0-9_]*`
<labelvalue>	Indicates a Unicode string.
<path>	Indicates the path of a valid URL.
<scheme>	Indicates a string that can use either "http" or "https" values.
<secret>	Indicates a normal string that should be kept secret, such as a password.
<string>	Indicates a regular string.

Note on PromQL expression

- Performance data obtained by PromQL statements described in metric definition files and alert configuration files must have the following labels set for each type of SID in the configuration information (for CloudWatchSIDs other than EC2, for each AWS namespace).

  For details about SID types of configuration information, see *3.15.6(1)(a) Type of SID of the target configuration and its available functions* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 2–118: Label that must be set in the performance data retrieved by the PromQL statement

Configuration information SID type	AWS namespace	Label that must be set in trend data (obtained with PromQL specified in promql in the metric definition file)	Label that must be set to alert (obtained with PromQL specified in expr in alert configuration file)
Agent SID	--	• instance • job • jp1_pc_nodelabel • jp1_pc_prome_hostname	• instance • job • jp1_pc_nodelabel • jp1_pc_exporter
Remote Agent SID			• instance • job • jp1_pc_nodelabel • jp1_pc_exporter • jp1_pc_remote_monitor_instance
CloudWatchSID for EC2	AWS/EC2		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_InstanceId
CloudWatchSID other than EC2	AWS/DynamoDB		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_TableName
	AWS/Lambda		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_FunctionName
	AWS/S3		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_BucketName • dimension_StorageType
	AWS/SQS		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_QueueName
	AWS/States		In addition to the common label# of CloudWatchSID, the following label is required. • dimension_APIName
SIDs to monitor logs	--	• instance • jp1_pc_nodelabel	--

(Legend)

--: N/A

#

The CloudWatchSID common label indicates the following labels:

- instance
- job
- jp1_pc_nodelabel
- jp1_pc_exporter
- account_id
- region
- jp1_pc_remote_monitor_instance

- When narrowing down performance data using without clauses, by clauses, etc. in PromQL statements, perform the narrowing down so that the labels described in "*Table 2-5 Labels that must be set in the performance data obtained by PromQL statements*" are not deleted.
- If an invalid PromQL statement is set in the promql of the metric definition file, the correct trend data will not be returned by the return trend data function.
- If an incorrect PromQL statement is set in expr in the alert configuration file, JP1 events may not be issued, extended attribute values may be blank, or JP1 events may not be associated with the correct IM management node.jpc_file_sd_config_node.yml

3 JP1 Events

This chapter describes the types and attributes of the JP1 events that are issued by JP1/IM.

3.1 Attributes of JP1 events

This section describes the attributes of JP1 events. JP1 event attributes are categorized into basic attributes and extended attributes. This section provides a detailed description of each event.

3.1.1 Basic attributes

All JP1 events have basic attributes. This subsection provides a detailed description of the basic attributes of JP1 events.

Details of the basic attributes of JP1 events

The basic attributes are sometimes identified by prefixing their names with `B.`, such as `B.ID`. When it is necessary to use the prefix `B.`, information to that effect is provided in the manual.

Table 3–1: Basic attributes of JP1 events

Item	Attribute name	Description
Serial number	`SEQNO`	The order in which the JP1 event arrived at this event server, regardless of the source of the JP1 event.
Event ID	`ID`	An 8-byte value that indicates the source application program that issued the JP1 event and the nature of the event.
Extended event ID	`IDEXT`	Eight hexadecimal characters that indicate the extended part of an event ID
Type	`TYPE`	Event type
Reason for registration	`REASON`	Reason why this JP1 event was registered in this event server.
Source process ID	`PROCESSID`	Process ID of the source application program.
Registered time	`TIME`	Time the JP1 event was registered at the source event server.
Arrived time	`ARRIVEDTIME`	Time the JP1 event was registered at the local event server.
Source user ID	`USERID`	User ID of the source process. If this is an event from Windows, `-1` is set.
Source group ID	`GROUPID`	Group ID of the source process. If this is an event from Windows, `-1` is set.
Source user name	`USERNAME`	User name of the source process.
Source group name	`GROUPNAME`	Group name of the source process. If this is an event from Windows, a space is set.
Event-issuing server name	`SOURCESERVER`	Name of the event server that issued the event. If the event has been forwarded, such as from JP1/Base (agent) to JP1/IM - Manager (site manager) to JP1/IM - Manager (integrated manager), the event server name of the initial JP1/Base is set.
Target event server name	`DESTSERVER`	If the source application program explicitly specifies forwarding of the event to another event server, the name of that event server is set.
Source IP address	`SOURCEIPADDR`	IP address of the source event server (this value is not accurate if the transmission was via NAT (network address translation) or a proxy, or if the JP1 event was forwarded because of environment settings).
Target IP address	`DESTIPADDR`	IP address of the target event server (this value is not accurate if the transmission was via NAT (network address translation) or a proxy, or if the JP1 event was forwarded because of environment settings).
Source serial number	`SOURCESEQNO`	Serial number at the source host (this value is not changed by forwarding).
Code set	`CODESET`	Name of the character code set that is used for messages, detailed information, and extended attributes.

Item	Attribute name	Description
Message	MESSAGE	Character string describing the details of the event.
Detailed information	--	Any data. Detailed information about basic attributes is usually used by a product that issues events that are compatible with JP1/SES version 5 or earlier in order to record detailed information. Products whose version is 6 or later typically use the JP1 event extended attributes to record detailed information.

Legend:

--: None

3.1.2 Extended attributes

Extended attributes are attributes that can be specified by a program that issues JP1 events. Extended attributes provide two types of information: common information and program-specific information. Common information is information that is common to all JP1 programs. Program-specific information applies to extended attributes that do not provide common information. This subsection provides a detailed description of common information.

Details of common information

The extended attributes are sometimes identified by prefixing their names with `E.`, such as `E.SEVERITY`. When it is necessary to use the prefix `E.`, information to that effect is provided in the manual.

The following table lists and describes the common information provided by extended attributes.

Table 3–2: List of common information provided by extended attributes

Item	Attribute name	Description
Event level	SEVERITY	Severity of the JP1 event. The following values can be assigned (listed here in descending order of severity): Emergency Alert Critical Error Warning Notice Information Debug
User name	USER_NAME	Name of the user executing the job.
Product name	PRODUCT_NAME	Name of the program that issued the JP1 event, such as the following: /HITACHI/JP1/AJS /HITACHI/JP1/FTP /HITACHI/JP1/NETMDM /HITACHI/JP1/NPS /HITACHI/JP1/NT_LOGTRAP /HITACHI/JP1/PAM /HITACHI/JP1/IM/SCOPE
Object type	OBJECT_TYPE	Name indicating the type of object that resulted in issuance of the event, such as the following: JOB, JOBNET, BATCHJOB, ACTION, LIST

Item	Attribute name	Description
Object name	OBJECT_NAME	Name of the object that resulted in issuance of the event (such as the name of a job or a jobnet).
Root object type	ROOT_OBJECT_TYPE	Type of object. This is usually the same as the object type, but in the case of an object that has a hierarchical structure, such as a jobnet, this indicates the object type at the highest level of the hierarchy. The permissible values are the same as for the object type.
Root object name	ROOT_OBJECT_NAME	Name used to issue an execution instruction during user operation. This is usually the same as the object name, but in the case of an object that has a hierarchical structure, such as a jobnet, this indicates the name of the object at the highest level of the hierarchy.
Object ID	OBJECT_ID	Object ID. Character string that uniquely identifies an object instance within the integrated system when it is combined with PRODUCT_NAME (the format depends on the product; this information is used to call the monitor of each product from the Tool Launcher window of JP1/IM - View).
Occurrence	OCCURRENCE	Event that occurred in the object indicated by the object name. The events include the following: START (Start of execution) END (End of execution) PAUSE (Pausing execution) RELEASE (Release of temporary stop) RESTART (Start of re-execution) CREATE (Creation of definition) DESTROY (Deletion of definition)
Start time	START_TIME	Execution or re-execution start time (absolute time in seconds since UTC 1970-01-01 00:00:0). This item might not be set.
End time	END_TIME	Execution end time (absolute time in seconds since UTC 1970-01-01 00:00:0). This item might not always be available to set.
Result code	RESULT_CODE	Termination code as a decimal character string. This item might not always be available to set.
Source host name	JP1_SOURCEHOST	Name of the source host.

3.2 JP1 events issued by JP1/IM

This section describes the JP1 events that are issued by JP1/IM.

3.2.1 List of JP1 events issued by JP1/IM - Manager

Event ID	When issued	Message	Function that issues the event
`00002010`	When an action's execution time exceeds the action delay monitoring time.	`KAVB4400-E The run time of an action for an event exceeded the action delay monitoring time.(Event_ID=`*event-ID*`, SEQNO=`*serial-number-in-event-database*`, Execution Host=`*action-execution-host*`, Action Serial Number=`*action-serial-number*`) Delay monitoring notifications will not be sent until suppression of the function for sending notifications to the action delay monitor is canceled.`	Automatic Action Service
`00002011`	When an action is placed in `Fail` or `Error` status while the action's status is being monitored.	`KAVB4402-E An event status is abnormal.(event ID = `*event-ID*`, event serial number = `*serial-number-in-event-database*`, execution host = `*action-execution-host*`, action serial number = `*action-serial-number*`) Status monitoring notifications will not be sent until suppression of the function for sending notifications to the action status monitor is canceled`	Automatic Action Service
`00002012`	When the health check function detects an error.	`KAVB8060-E An abnormality was detected in `*function-name*`. (host name = `*host-name*`, process name = `*process-name*`, process ID = `*process-ID*`) : `*maintenance-information*	• Event Console Service • Event Base Service
`00002013`[#1]	When the health check function detects an error.	`KAVB8062-E An abnormality was detected in `*function-name*`. (host name = `*host-name*`, process name = `*process-name*`) : `*maintenance-information*	Event Console Service
`00002014`[#2]	When the health check function detects error recovery.	`KAVB8061-I `*function-name*` has been recovered. (host name = `*host-name*`, process name = `*process-name*`, process ID = `*process-ID*`) : `*maintenance-information*	• Event Console Service • Event Base Service
`00002015`	When suppression of the function for sending notification to the action delay monitor is released.	`KAVB4401-I Suppression of the function for sending notifications to the action delay monitor was canceled.`	Automatic Action Service
`00002016`	When suppression of the function for sending notification to the action status monitor is released.	`KAVB4403-I Suppression of the function for sending notifications to the action status monitor was canceled.`	Automatic Action Service
`00002020`	When an action that has been placed in delayed status during action delay monitoring	`KAVB4404-E Although the run time of an action exceeded the action delay monitoring time, an action delay notification event could not be sent`	Automatic Action Service

Event ID	When issued	Message	Function that issues the event
	wraps around in the action information file.	`because no action information exists in the action information file. (action serial number =` *action-serial-number*`) Delay monitoring notifications will not be sent until suppression of the function for sending notifications to the action delay monitor is canceled.`	
`00002021`	When an action that has been placed in error status during action status monitoring wraps around in the action information file.	`KAVB4405-E Although an action status is abnormal, an action state notification event could not be sent because no action information exists in the action information file. Status monitoring notifications will not be sent until suppression of the function for sending notifications to the action status monitor is canceled.:` *maintenance-information*	Automatic Action Service
`000020A0`	When automated action processing terminates abnormally due to a problem that prevents processing from resuming.	`KAVB4054-E Automatic Action was terminated abnormally. (Hostname :` *host-name*`)`	Automatic Action Service
`000020A1`	When an automated action is started by the `jco_start(.model)` command. The default is that this event is not issued.	`KAVB4050-I Automatic Action was started. :` *logical-host-name*	Automatic Action Service
`000020A2`	When an automated action is terminated by the `jco_stop(.model)` command. The default is that this event is not issued.	`KAVB4051-I Automatic Action was terminated. :` *logical-host-name*	Automatic Action Service
`000020A3`	When the automated action function is started by the `jcachange` command or by a window operation.	`KAVB4055-I The action definition file was read and the automatic action function status was changed to operating. The processing will be based on the definitions read from the subsequently received (`*arrival-time-of-most-recently-processed-event* `(`*YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*`)) events. (Definition=`*total-number-of-effective-definitions*`/`*total-number-of-definitions-in-file*`, SEQNO=`*serial-number-of-most-recently-processed-event*`)`	Event Base Service
`000020A4`	When the status of the automated action function changes from running to standby.	`KAVB4056-I Automatic action was suspended. Automatic actions cannot be executed for the subsequently received (`*arrival-time-of-most-recently-processed-event* `(`*YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*`)) events. (SEQNO=`*serial-number-of-most-recently-processed-event*`)`	Event Base Service
`000020A5`	When setting of locale information by Automatic Action Service fails.	`KAVB4909-E An attempt to set locale information has failed.`	Automatic Action Service

Event ID	When issued	Message	Function that issues the event
000020A6	When setting of locale information by the Event Base Service process fails.	KAVB4909-E An attempt to set locale information has failed.	Event Base Service
000020E0	When execution of an action starts.	KAVB4430-I Execution of the action for an event was requested. (Event_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)	Automatic Action Service
000020E1	When execution of an action is completed.	KAVB4431-I Execution of the action for an event ended normally. (EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*, Return_code=*termination-code*)	Automatic Action Service
000020E2	When an automated action or an action under command control is placed in abnormal status.	KAVB4432-E Automatic action or command control of the action for an event ended abnormally.(EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)	Automatic Action Service
000020E3[#3]	When an action execution request for an action status notification event is registered.	KAVB4433-I Execution of the action for an action state notification event was requested.(Event_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)	Automatic Action Service
000020E4[#3]	When an action for an action status notification event terminates.	KAVB4434-I Execution of the action for an action state notification event ended normally. (EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*, Return_code=*termination-code*)	Automatic Action Service
000020E5[#3]	When an automated action or an action under command control for an action status notification event is placed in abnormal status.	KAVB4435-E Automatic action or command control of the action for an action state notification event ended abnormally.(EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)	Automatic Action Service
000020E6[#3]	When the jcocmddef command has been set to provide notification of execution requests, but issuance of the action status notification event (000020E0 or 000020E3) for an execution request fails because the action information file has wrapped around. (Event level: Warning).	KAVB4436-W Although Execution of the action for an event was requested, an action state notification event could not be sent because no action information exists in the action information file. : *maintenance-information*	Automatic Action Service
000020E7[#3]	When the jcocmddef command has been set to provide notification of command execution terminations, but issuance of the action status notification event (000020E1 or 000020E4) for an execution termination fails because the action	KAVB4437-W Although Execution of the action for an event ended normally, an action state notification event could not be sent because no action information exists in the action information file. : *maintenance-information*	Automatic Action Service

Event ID	When issued	Message	Function that issues the event
	information file has wrapped around. (Event level: `Warning`).		
`000020E8`#3	When the `jcocmddef` command has been set to provide notifications of abnormal command terminations, but issuance of the action status notification event (`000020E2` or `000020E5`) for an abnormal termination fails because the action information file has wrapped around. (Event level: `Error`).	`KAVB4438-E Although automatic action or command control of the action for an event ended abnormally, an action state notification event could not be sent because no action information exists in the action information file. :` *maintenance-information*	Automatic Action Service

`00003F01`#1	When no more events can be displayed because there are no events to be acquired from the event buffer at the connected host.	`KAVB1513-W Cannot display some event(S).`
		`There were no events to obtain from the event buffer on the connecting host.`
		`All the events except the above will be displayed.`
		`To search for an event which was not displayed, specify the search conditions in the event search condition settings dialog as follows:`
		`(1) In "Search host", specify the name of the connecting host.`
		`(2) In "Registered timeframe", specify the times when the events before and after this event were registered.`
		`Check to see if the following conditions are met when this event appears frequently.`
		`(1) The "Interval" value that was set for "Automatic refresh" in the Preferences window is too long.`
		`(2) The "Num. of events to acquire at update" value that was set in the Preferences window is too small.`
		`(3) The "Event buffer" value for the Manager that was set in the System Environment Settings window is too small.`
			Event Console Service

`00003F02`#1	When the event is not found in the event buffer on the connected host, and the event cannot be displayed either on the **Monitor Events** page or the **Severe Events** page, displays the event you want to obtain on the applicable page. To display it on the **Severe**	`KAVB1540-W Cannot display some event(s). (page =` *page*`).`
		`There were no events to obtain from the event buffer on the connecting host.`
		`All the events except the above will be displayed.`
		`To search for an event which was not displayed, specify the search`
			Event Console Service

Event ID	When issued	Message	Function that issues the event
	Events page, forcibly treat the event as a severe event.	conditions in the event search condition settings dialog as follows: (1) In "Search host", specify the name of the connecting host. (2) In "Registered timeframe", specify the times when the events before and after this event were registered. Check to see if the following conditions are met when this event appears frequently. (1) The "Interval" value that was set for "Automatic refresh" in the Preferences window is too long. (2) The "Num. of events to acquire at update" value that was set in the Preferences window is too small. (3) The "Event buffer" value for the Manager that was set in the System Environment Settings window is too small.	
00003F03[#1]	When an error occurs while events are being acquired from Event Service.	KAVB1516-W An error occurred in acquiring an event from the event service. Cannot recover the error after attempting the number of retries specified in the system profile. No more events will be displayed from now on due to this error. Please check if the event service is running or not. If not, recover the error by re-executing the manager after starting the event service.	Event Console Service
00003F04[#1]	When an attempt is made to search for events using a condition that is not supported for the Event Service of JP1/Base version 06-00 (such as Is contained, Is not contained, Regular expression, or specification of multiple action statuses) or JP1/Base version 06-51 (such as Regular expression).	KAVB1527-E A condition that cannot be received by the search host is included.	Event Console Service
00003F05[#1]	When the filter length is found to exceed Event Service's maximum value during event search processing.	KAVB0246-E The filter condition exceeds the maximum length. (Maximum length:*maximum-length*)	Event Console Service
00003F06[#1]	When a specified regular expression is found to be invalid during event search processing.	KAVB0248-E The settings for a regular expression is incorrect.	Event Console Service

Event ID	When issued	Message	Function that issues the event
00003F07[#1]	When the connection between Event Base Service and Event Service is lost.	KAVB4764-W An error occurred in acquiring an event from the event service. Please check if the event service is running or not. If not, recover the error by starting the event service.	Event Base Service
00003F08[#1]	When an attempt is made to execute an event search with an exclusion-condition specified, but the search host's JP1/Base version is 08-11 or earlier.	KAVB0251-E The search cannot be performed for the specified condition because the search host's JP1/Base does not support the exclusion condition.	Event Console Service
00003F11	When the status of a JP1 event action is changed by an operation in one of the following windows or by entering the following command: • Event Console window • Related Events window • jcochstat command • When there is a response for a response-waiting event and the status of the response-waiting event is changed to Processed • When a response-waiting event is canceled by BJEX or JP1/AS, and the status of the response-waiting event is changed to Processed	KAVB1577-I A status operation was performed. (user who performed the operation = *JP1-user*, event ID = *event-ID*, status before operation = *status-before-operation*, status after operation = *status-after-operation*)	Event Console Service
00003F13[#4]	When a message is issued that provides notification that an event acquisition filter condition of JP1/IM - Manager has been changed in the System Environment Settings window or the Event Acquisition Conditions List window, or by entry of the jcochfilter command.	KAVB4014-I The event acquisition filter definition file was read. The read definitions will be used for processing from the next received event. (filter name = *filter-name*, last received event = *arrival-time*, serial number in event DB = *serial-number-in-event-DB*)	Event Base Service
Event ID specified in the SUCCESS_EVENT parameter in the correlation event generation definition file	When a specified correlation event generation condition results in success during correlation event generation processing.	Message specified in the FAIL_EVENT parameter in the correlation event generation definition file	Correlation event generation function

Event ID	When issued	Message	Function that issues the event
Event ID specified in the `FAIL_EVENT` parameter in the correlation event generation definition file	When a specified correlation event generation condition results in failure during correlation event generation processing.	Message specified in the `SUCCESS_EVENT` parameter in the correlation event generation definition file	Correlation event generation function
`00003F15`	When the integrated monitoring database is enabled and a message is sent providing notification that the severe event definition of JP1/IM - Manager (Central Console) has been changed from the Severe Event Definitions window.	`KAVB1669-I The severe event definition file has been read. Next, processing will be performed using the definition read from the acquired event. (Event acquired at the end:Arrival time =` *arrival-time-of-the-event-acquired-at-the-end*`, serial number in event DB =` *serial-number-in-event-database-of-the-event-acquired-at-the-end*`)`	Event Base Service

`00003F16`[#1]	When an error occurs while events are being acquired from the integrated monitoring database.	`KAVB1671-W An error occurred in acquiring an event from the integrated monitoring database.`
		`Cannot recover the error after attempting the number of retries specified in the system profile.`
		`No more events will be displayed from now on due to this error.`
			Event Console Service

`00003F17`[#4]	When a message is issued providing notification that additional common exclusion-conditions have been registered from JP1/IM - View.	`KAVB1150-I An additional common exclusion conditions group was registered. (common exclusion conditions group ID =` *common-exclusion-conditions-group-ID*`, common exclude conditions group name =` *common-exclude-conditions-group-name*`, registering user =` *user-name*`)`	Event Base Service
`00003F20`[#4]	When a message is issued providing notification that an event acquisition filter condition of JP1/IM - Manager (Event Generation Service) has been changed in the System Environment Settings window or the Event Acquisition Conditions List window, or by entry of the `jcochfilter` command.	`KAJV2179-I The event acquisition filter definition file was read. The read definitions will be used for processing from the next received event. (filter name =` *filter-name*`, last received event =` *arrival-time*`, serial number in event DB =` *serial-number-in-event-database*`)`	Event Generation Service
`00003F21`	When a message is issued providing notification that a correlation event generation definition has been updated by the `jcoegschange` command.	`KAJV2242-I The correlation event generation definition file has been read, and the definitions for the correlation event generation function have been updated. (file name =` *file-name*`)`	Event Generation Service
`00003F22`	When the setting for regular expressions used for JP1/Base at JP1/IM - Manager startup is	`KAVB4712-W The event base service cannot use common exclusion condition groups (extended) because a regular expression used by JP1/Base is not`	Event Console Service

Event ID	When issued	Message	Function that issues the event
	not extended regular expressions, and the operating mode of the common exclusion-conditions group for JP1/IM - Manager is set to extended mode	`extended. The event base service will start without any common exclusion condition groups (extended) being set.`	
`00003F23`	When the setting for regular expressions used for JP1/Base at JP1/IM - Manager startup is not extended regular expressions, and the operating mode of the common exclusion-conditions group for JP1/IM - Manager is set to extended mode	`KAJV2502-W The correlation event issuing service cannot use common exclusion condition groups (extended) because the regular expressions used by JP1/Base are not extended. The correlation event issuing service will start without any common exclusion condition groups (extended) being set.`	Event Correlation Feature
`00003F25`	When a message is issued providing notification that correlation event generation processing has been restarted by the `jcoegsstart` command.	`KAJV2243-I The correlation event generation function has been restarted.`	Event Generation Service
`00003F26`	When a message is issued providing notification that correlation event generation processing has been terminated by the `jcoegsstop` command without stopping the Event Generation Service.	`KAJV2234-I The correlation event generation function has stopped.`	Event Generation Service
`00003F28`	When the number of JP1 event sets issued by the Event Generation Service exceeds the maximum value (20,000 sets).	`KAJV2322-W A JP1 event (event ID =` *event-ID*`, serial number in the event database =` *serial-number-in-event-database*`) could not be correlated because the number of correlated JP1 event pairs has reached the upper limit (20,000).`	Event Generation Service
`00003F31`[#4]	When a message is issued providing notification that additional common exclusion-conditions have been registered from JP1/IM - View	`KAJV2188-I An additional common exclusion conditions group was registered. (common exclusion conditions group ID =` *common-exclusion-conditions-group-ID*, `common exclude conditions group name =` *common-exclude-conditions-group-name*, registering user = *user-name*)	Event Generation Service
`00003F41`	When more response-waiting events than the maximum that can be accumulated have been issued.	`KAVB0551-E The number of accumulated response-waiting events on the manager exceeded the maximum (2000).`	Event Console Service

`00003F42`	When response-waiting data for the file for accumulated response-waiting events cannot be read.	`KAVB1816-W A response-waiting event could not be displayed.`
		`To search for the event, specify the search conditions in the dialog`
			Event Console Service

Event ID	When issued	Message	Function that issues the event
		box for setting the event search conditions as follows: (1) As the host to be searched for, specify the name of the connected host. (2) As the response-waiting event, specify the target event. (3) As the arrival timeframe, specify the times when the events before and after this event arrived.	
00003F51	When events are deleted from the integrated monitoring database.	KAVB1841-I The events from *deletion-target-start-date-and-time* to *deletion-target-end-date-and-time* were deleted from the integrated monitoring database.	Integrated monitoring database
00003F52	When the number of events on which an output-and-save operation has not been performed exceeds the deletion warning position.	KAVB1842-W Events not output for preservation have exceeded the deletion warning level (*deletion-warning-level*%).	Output-and-save function
00003F53[#1]	When an error occurs while events are being registered into the integrated monitoring database.	KAVB1832-E An error occur while attempting to register an event into the integrated monitoring database. The system will retry registering the event. (detailed information = *detailed-information*)	Event Base Service
00003F54	When an event registration error that occurred in the integrated monitoring database is recovered.	KAVB1833-I An error occur while attempting to register an event into the integrated monitoring database. However, after several retries, the event was registered into the database. The event base service is restarting event acquisition.	Event Base Service
00003F56[#4]	When an additional repetition event condition has been registered (added).	KAVB4673-I A repeated event condition was registered. (repeated event condition name = *repeated-event-condition-name*, registering user = *user-name*)	Repeated event monitoring suppression function
00003F57[#4]	When the **Apply** button in the List of Repeated Event Conditions is clicked.	KAVB4674-I The definition file for the repeated event condition was updated. Next, processing will be performed using the definition read from the received event. (arrival time of the last received event = *arrival-time-of-the-last-received-event*, serial number in the event database = *serial-number-in-the-event-database*)	Repeated event monitoring suppression function
00003F58	When suppression of the repeated event monitoring suppression function starts.	KAVB4676-I Suppression of repeated events that match the repeated event condition (*repeated-event-condition-name*) has started. (arrival time of the first suppressed event = *arrival-time-of-the-first-suppressed-event*, event database serial number of the first suppressed event = *event-database-serial-number-of-the-first-suppressed-event*)	Repeated event monitoring suppression function

Event ID	When issued	Message	Function that issues the event
`00003F59`	When suppression of the repeated event monitoring suppression function ends.	`KAVB4677-I Suppression of repeated events that match the repeated event condition (`*repeated-event-condition-name*`) has ended. (arrival time of the suppressed event = `*arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* `-` *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*`, event database serial number of the suppressed event = `*event-database-serial-number-of-the-first-suppressed-event* `-` *event-database-serial-number-of-the-last-suppressed-event*`)`	Repeated event monitoring suppression function
`00003F60`	When suppression of monitoring repeated events has ended	`KAVB4678-I Suppression of repeated events that match the repeated event condition (`*repeated-event-condition-name*`) has terminated. (arrival time of the suppressed event = `*arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* `-` *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*`, event database serial number of the suppressed event = `*event-database-serial-number-of-the-first-suppressed-event* `-` *event-database-serial-number-of-the-last-suppressed-event*`)`	Repeated event monitoring suppression function
`00003F61`	When a severity changing definition has been applied and `jco_spmd_reload` is executed.	`KAVB4600-I The severity change definition has been read. Next, processing will be performed using the definition read from the received event. (arrival time of the last received event = `*arrival-time*`, serial number in the event database = `*serial-number-in-event-database*`)`	Event Base Service
`00003F63`	When the event source host mapping definition is applied. When `jco_spmd_reload` is executed.	`KAVB4650-I An event-source-host mapping definition was read. Processing will be performed by the definition read from the next received event. (last received event: reception time = `*reception-time*`, event database serial number = `*event-database-serial-number*`)`	Event source host mapping feature
`00003F64`	When a business group is updated	`KAVB8453-I The business group was updated. Processing will be performed from the next-received event. (last received event: reception time = `*reception-time*`, event database serial number = `*event-database-serial-number*)	Restriction on referencing and operating business groups
`00003F65`	When suppression of monitoring repeated events is regarded as continued	`KAVB4679-I Suppression of repeated events that match the repeated event condition (`*repeated-event-condition-name*`) will continue. (arrival time of the suppressed event = `*arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* `-` *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*`, event database serial number of the suppressed event = `*event-database-*	Repeated event monitoring suppression function

Event ID	When issued	Message	Function that issues the event
		serial-number-of-the-first-suppressed-event - *event-database-serial-number-of-the-last-suppressed-event*)	
00003F68	When a business group is updated	KAVB8454-W The business group could not be updated. (cause = *cause*)	Restriction on referencing and operating business groups
00003F69	When a business group is updated	KAVB8456-E The business group could not be updated. (cause = *cause*)	Restriction on referencing and operating business groups
00003F6A	When a display message change definition is applied. When jco_spmd_reload is executed.	KAVB4623-I The display message change definition has been read. Next, processing will be performed using the definition read from the received event. (arrival time of the last received event = *arrival-time*, serial number in the event database = *event-database-serial-number*)	Display message change function
00003F71	When the additional severity changing definition is registered	KAVB4802-I A severity change definition was registered. (severity change definition name = *severity-change-definition-name*, registered user = *user-name*)	Severity change function of events
00003F76	When an additional display message change definition is registered	KAVB4803-I A display message change definition was registered. (display message change definition name = *display-message-change-definition-name*, registering user = *user-name*)	Display message change function
00003F77	When a definition file for extended event attributes is reloaded	KAVB5800-I The definition file for extended event attributes was read in to JP1/IM - Manager.	Function for displaying and specifying program-specific extended attributes
00003F78	When a definition file for extended event attributes is reloaded, but some of the definition file fails to reload	KAVB5804-E An attempt to read the definition file for extended event attributes failed because part of the definition file for extended event attributes could not be read.	Function for displaying and specifying program-specific extended attributes
00003F7C	When a definition file for opening monitor windows is reloaded	KAVB1981-I The definition file for opening monitor windows was applied to JP1/IM - Manager.	Monitor startup of linked products
00003FA0#5	When command execution control receives a command execution request from the Execute Command window.	KAVB2100-I [*host-name*:*JP1-user-name*] Command execution started.	JP1/Base command execution
00003FA1#5	When execution of a command requested from the Execute Command window is completed.	KAVB2101-I [*host-name*:*JP1-user-name*] Command execution ended normally.	JP1/Base command execution
00003FA2#5	When it is detected that a command whose execution was requested from the Execute Command	KAVB2102-E [*host-name*:*JP1-user-name*] Command execution ended abnormally.	JP1/Base command execution

Event ID	When issued	Message	Function that issues the event
	window cannot be executed for some reason.		
`00003FA3`#5	When execution of a command was requested from the Execute Command window but the elapsed time event issuance interval for the automated action is exceeded. (The `jcocmddef` command is used to specify the elapsed time event issuance interval).	`KAVB2402-W [`*host-name*`]The execution time of command execution exceeded the regulation value (`*numeric-value*` sec)`	JP1/Base command execution
`00003FA5`#5	When the number of pre-loaded automated actions reaches a threshold value (if a threshold for the number of pre-loaded commands has been set by the `jcocmddef` command).	`KAVB2071-W In `*target-host-name*`, the number of queued commands requested from `*source-host-name*` has exceeded the threshold (`*xx*`).`	JP1/Base command execution
`00003FA6`#5	When the number of pre-loaded automated actions becomes 0 (if a threshold for the number of pre-loaded commands has been set by the `jcocmddef` command).	`KAVB2072-I In `*target-host-name*`, the number of queued commands requested from `*source-host-name*` has become 0.`	JP1/Base command execution
`00003FB0`	When the status of a monitoring node changes.	`KAVB7900-I Status of `*monitoring-node-name*` is changed `*status*` from `*status*`.`	Central Scope Service
`00003FB1`	When the number of monitoring node status change events reaches a maximum value.	`KAVB7901-W The number of status change event for the monitored node `*monitoring-node-ID*` has reached the threshold.`	Central Scope Service
`00003FC0`	When a remote monitoring log-file trap is unable to start monitoring a log file.	`KNAN26102-E The remote log-file trap cannot start. (Code: `*code*`, Host name: `*host name*`, Monitoring-target-name: `*monitoring-target-name*`)`	Remote monitoring feature
`00003FC1`	When the number of retries for reading a remote monitoring log-file trap exceeds the threshold, and monitoring of the applicable log file has stopped.	`KNAN26094-E The relevant log file could not be read after the specified number of retires, so monitoring will stop. (Code: `*code*`, Host name: `*host-name*`, Monitoring-target-name: `*monitoring-target-name*`, Log file name: `*Log file name*`)`	Remote monitoring feature
`00003FC2`	When the status of a remote monitoring log-file trap changes to abnormal.	`KNAN26095-E The relevant log file can no longer be monitored. (Code: `*code*`, Host name: `*host-name*`, Monitoring-target-name: `*monitoring-target-name*`, Log file name: `*Log file name*`)`	Remote monitoring feature
`00003FC3`	When a remote monitoring log-file trap terminates abnormally.	`KNAN26057-E The remote log-file trap will stop due to error. (Code:`	Remote monitoring feature

Event ID	When issued	Message	Function that issues the event
		code, Host name: *host name*, Monitoring-target-name: *monitoring-target-name*)	
00003FC5	When the amount of data for a log file collected by a remote monitoring log-file trap exceeds the allowed upper limit for logs.	KNAN26140-W The amount of data that a remote log file trap collected from the log file exceeded the limit. The log entries output from the last collection time to this collection time will not be output as JP1 events. (host name: *host name*, monitoring-target name: *monitoring-target-name*, log file name: *Log file name*, previous collection time: *Last collection time*(*yyyy/MM/dd hh:mm:ss*), this collection time: *This collection time*(*yyyy/MM/dd hh:mm:ss*))	Remote monitoring feature
00003FC6	When a remote monitoring log-file trap stops as a result of executing the collection of host information on the monitored host where remote monitoring is running	KNAN26351-E All trapping of remote log files on monitored host "*monitored-host-name*" will now stop. (cause = *cause*)	Remote monitoring feature
00003FC7	When a renamed log file (backup file) cannot be found (only when the SEQ2 format is used and the monitored host is a UNIX host)	KNAN26350-W The backup files for the monitored log files were not found. The log entries output to the backup files between the previous collection time and the current collection time will not be output as JP1 events. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*, log file name = *monitored-log-file-name*, previous collection time = *yyyy/MM/dd hh*:*mm*:*ss*, current collection time = *yyyy*/*MM*/*dd hh*:*mm*:*ss*, user = *user*, command line that was executed = *command-line-executed*)	Remote monitoring feature
00003FC8	When a renamed log file (backup file) cannot be found (only when the SEQ2 format is used and the monitored host is a Windows host)	KNAN26352-W The backup files for the monitored log files were not found. The log entries output to the backup files between the previous collection time and the current collection time will not be output as JP1 events. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*, log file name = *monitored-log-file-name*, previous collection time = *yyyy*/*MM*/*dd hh*:*mm*:*ss*, current collection time = *yyyy*/*MM*/*dd hh*:*mm*:*ss*, user = *user*)	Remote monitoring feature
00003FC9	When a remote monitoring event log trap trap stops as a result of executing the collection of host information on the monitored host where remote monitoring is running	KNAN26353-E Trapping of remote event log files on monitored host "*monitored-host-name*" will now stop. (cause = *cause*)	Remote monitoring feature

Event ID	When issued	Message	Function that issues the event
00003FD0	When a remote monitoring event log trap is unable to start monitoring Windows events.	KNAN26107-E The remote event-log trap cannot start. (Code: *code*, Host name: *host name*)	Remote monitoring feature
00003FD1	When the number of retries for reading an event log trap for remote monitoring exceeds the threshold, and monitoring of the applicable Windows events stops.	KNAN26028-E Monitoring will now stop because the event log could not be read after the specified number of retries. (Code: *code*, Host name: *host name*)	Remote monitoring feature
00003FD2	When reading of an event log file is retried.	KNAN26027-I The system will now retry reading the event log. (Code: *code*, Host name: *host name*)	Remote monitoring feature
00003FD3	When a remote monitoring event log trap terminates abnormally.	KNAN26002-E The remote event-log trap will now stop due to error. (Code: *code*, Host name: *host name*)	Remote monitoring feature
00003FD4	When reading of an event log is successful on a retry.	KNAN26026-I An event log can now be monitored. (Host name: *host name*)	Remote monitoring feature
00003FD5	When the differing-components data for an event log collected by a remote monitoring event log trap exceeds the upper limit for logs.	KNAN26142-W The amount of data collected from the host by a remote event-log trap exceeded the limit. The event log entries that were output during the period from the previous collection time to the current collection time will not be output as JP1 events. (host name = *host-name*, previous collection time = *previous-collection-time*, current collection time = *current-collection-time*)	Remote monitoring feature
00003FD6	When an operation to write to the remote monitoring status retention file by the remote-monitoring log file trap fails.	KNAN26339-W Failed to save the state of the remote log file trap when the log was collected. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*)	Remote monitoring feature
00003FD7	When an operation to write to the remote monitoring status retention file by the remote-monitoring event log trap fails.	KNAN26340-W Failed to save the state of the remote event log trap when the log was collected. (host name = *monitored-host-name*)	Remote monitoring feature
00003FD8	When an operation to read the remote monitoring status retention file by the remote-monitoring log file trap fails.	KNAN26341-W Failed to restore the remote log file trap to its state when it was last terminated. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*)	Remote monitoring feature
00003FD9	When an operation to read the remote monitoring status retention file by the remote-monitoring event log trap fails.	KNAN26342-W Failed to restore the remote log file trap to its state when it was last terminated. (host name = *monitored-host-name*)	Remote monitoring feature
00003FDA	When the logs output while remote monitoring was stopped cannot be collected	KNAN26343-W The remote log file trap was not restored to its state when it was last terminated, because the	Remote monitoring feature

Event ID	When issued	Message	Function that issues the event
	after remote monitoring resumes (warm start) because a monitored log was changed by a remote-monitoring log file trap.	`trap was in a state where it could not be monitored. (details =` *detailed-information*`, host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`, log file name =` *log-file-name*`)`	
`00003FDB`	When the system recovers from an error in the operation to write to the remote monitoring status retention file by the remote-monitoring log file trap.	`KNAN26345-I An error in the processing to save the state of the remote log file trap that occurred during log collection was resolved. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`	Remote monitoring feature
`00003FDC`	When the system recovers from an error in the operation to write to the remote monitoring status retention file by the remote-monitoring event log trap.	`KNAN26346-I An error in the processing to save the state of the remote event log trap that occurred during log collection was resolved. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`	Remote monitoring feature
Value specified for the `ACTDEF` parameter[#6]	When an AP log file record is detected.	Data content of one line in a log file	Remote monitoring feature
Details of `00003A71`, or the event ID specified in the filter block of the remote-monitoring event log trap action-definition file[#7]	When a log message reporting a Windows event is detected.	Event log message	Remote monitoring feature
`00003F90`[#8]	When a process terminates abnormally.	`KAVB3737-E The` *component-name managed-process-name* `terminated abnormally.`	JP1/IM - Manager process management
`00003F91`[#8]	When a timeout occurs during process startup.	`KAVB3613-W A` *component-name* `timeout occurred in` *managed-process-name*`. Processing continues.`	JP1/IM - Manager process management
`00003F92`[#8]	When a process that terminated abnormally restarts.	`KAVB3616-I Restart of the` *component-name managed-process-name* `has finished.`	JP1/IM - Manager process management
`00006400`[#9]	When a display message change event is issued	If the message was changed by the display message change function, the changed message is set. If the message was not changed, the message text of the original event is set.	Issuance of a display message change event
`00003FE0`	When the response action starts	`KAJY22023-I The response action will now start. (suggestion ID :` *suggestion-ID*`, JP1 user name :` *JP1-user-name*`, IM management node :` *tree-SID*`, action information :` *action-information*`)`	Suggestion function provided by JP1/IM - Manager (Intelligent Integrated Management Base)
`00003FE1`	When the response action ends	`KAJY22024-I The response action has finished. (suggestion ID :` *suggestion-ID*`, JP1 user name :` *JP1-user-name*`, IM management node :` *tree-SID*`, action information :` *action-information*`)`	Suggestion function provided by JP1/IM - Manager (Intelligent Integrated Management Base)

Event ID	When issued	Message	Function that issues the event
00003FE2	When the execution of the response action failed	KAJY22025-E Execution of the response action failed. (suggestion ID : *suggestion-ID*, JP1 user name : *JP1-user-name*, cause : *cause*, IM management node : *tree-SID*, action information : *action-information*)	Suggestion function provided by JP1/IM - Manager (Intelligent Integrated Management Base)
00003FF0	When Status of the auto Response Action is set to "Execute control sending"	KAJY63025-I Response Action for event. (Serial number in integrated monitoring DB = Serial number in integrated monitoring DB) was sent to JP1/IM-Manager managing Response Action Execute destination.	Auto execution of Response Action
00003FF1	When Status of Auto Response Action is set to "Queuing"	KAJY63026-I Response Action for event. (Serial number in the integrated monitoring DB = Serial number in the integrated monitoring DB) was requested to JP1/IM agent management base.	Auto execution of Response Action
00003FF2	When Status of Auto Response Action is set to "Exit"	KAJY63027-I Execution of Response Action for event. (Serial number in the integrated monitoring DB = Serial number in the integrated monitoring DB) has terminated. (End code = End code)	Auto execution of Response Action
00003FF3	When Status of Auto Response Action is "Fail", "Communication Failed", or "error"	KAJY63028-E Response Action for event. (Serial number in the integrated monitoring DB = Serial number in the integrated monitoring DB) terminated abnormally.	Auto execution of Response Action
00003FF4	When Status of the auto Response Action for Response Action notification event is set to "Execution control sending"	KAJY63029-I Response Action for Response Action Status notification event (serial number in integrated monitoring DB = serial number in integrated monitoring DB) was sent to JP1/IM-Manager managing Response Action Execute destination.	Auto execution of Response Action
00003FF5	When Status of auto Response Action for Response Action notification event is set to "Queuing"	KAJY63030-I Response Action for Response Action Status notification event (serial number in the integrated monitoring DB = serial number in the integrated monitoring DB) was requested to JP1/IM agent management base.	Auto execution of Response Action
00003FF6	When Status of the auto Response Action for Response Action notification events is set to "Exit"	KAJY63031-I Execute of Response Action for Response Action Status notification event (serial number in the integrated monitoring DB = serial number in the integrated monitoring DB) has terminated. (End code = End code)	Auto execution of Response Action
00003FF7	When Status of the auto Response Action for Response Action notification event is "Fail", "Communication Failed", or "Execute Failed"	KAJY63032-E Response Action for Response Action Status notification event (serial number in integrated monitoring DB = serial number in integrated monitoring DB) terminated abnormally.	Auto execution of Response Action
00003FF8	Failed to issue Response Action notification event (queuing)	KAJY63033-W Execution of Response Action was requested, but Response Action Status notification event cannot be issued because Response Action does not exist in Response Action results-management database. (Detailed Information : Detailed Information)	Auto execution of Response Action
00003FF9	Response Action notification event issuance failure (Execute termination)	KAJY63034-W Execution of Response Action has terminated, but Response Action Status notification event cannot be issued because Action does not	Auto execution of Response Action

Event ID	When issued	Message	Function that issues the event
		exist in Response Action results-management database. (Detailed Information : Detailed Information)	
00003FFA	Response Action notification event issue failure (Execute failure)	KAJY63035-E Response Action terminated abnormally, but Action Status notification event cannot be issued because there is no Action in Response Action results-management database. (Detailed Information : Detailed Information)	Auto execution of Response Action
00003FFB	When the auto Response Action defi nition is loaded and auto execution of Response Action goes to the operational Status	KAJY63023-I read Auto Response Action Definitions and set auto execution of Response Action to Operational Status. The definition read from the next received event is processed. (Number of definitions: Enable number of definitions/total number of definitions in definition, last received event: arrival time = arrival time of last processed event (YYYY/MM/DD HH:MM:SS), serial number in integrated monitoring DB = serial number in integrated monitoring DB of last processed event)	Auto execution of Response Action
3F80	When you have finished generating IM management node related information	KAJY02073-I Generation of the information related to IM management nodes ended normally.	Generating IM Management Node Related Information
3F81	Failure to generate IM management node-related information	KAJY02074-E Failed to generate the information related to IM management nodes. (return value = *return-value*, details = *details*)	Generating IM Management Node Related Information
3F82	When you have finished reflecting IM management node-related information	KAJY02075-I Processing to apply the information related to IM management nodes ended normally.	Reflecting IM Management Node Related Information
3F83	Failure to propagate IM management node-related information	KAJY02076-E Failed to apply the information related to IM management nodes. (return value = *return-value*, details = *details*)	Reflecting IM Management Node Related Information

#1: These are dummy events to which the following limitations apply:

- The event cannot be searched in the Event Console window.
- If the details of the event are displayed, the JP1 event basic and extended attributes are not displayed.
- No action is executed pursuant to such an event even if an automated action is set.
- No mapping is performed on the event even if event information mapping is defined.
- This event is not subject to monitor startup.
- This event is not subject to the event acquisition filter.
- This event is not subject to correlation event generation processing.
- This event is not registered in the event database. Therefore, when JP1/IM - Manager is restarted, this event is no longer displayed in the Event Console window.
- If you change the event action status, the changes are not applied to other parts of JP1/IM - View.

#2: When recovery of JP1/Base Event Service (`jevservice`) is detected, the following message is displayed: `KAVB8063-I`.

#3: The following limitation applies to these events:

- No action is executed on this event even if an automated action is set.

#4: The following limitation applies to these events:

- This event is not subject to the event acquisition filter.

#5: This is a JP1 event issued by JP1/Base command execution. For details about the JP1 events, see the chapter that describes JP1 events in the *JP1/Base User's Guide*.

#6: For details about JP1 events issued by log file traps of JP1/Base instead of the remote monitoring function, see the chapter describing JP1 events in the *JP1/Base User's Guide*.

#7: For details about JP1 events issued by log file traps of JP1/Base instead of the remote monitoring function, see the chapter describing JP1 events in the *JP1/Base User's Guide*.

#8: This event is issued only if issuance of JP1 events in response to process errors is set. To issue such JP1 events, you must edit the IM parameter definition file and then execute the `jbssetcnf` command. For details about definition files, see *IM parameter definition file (jp1co_param_V7.conf)* in *Chapter 2. Definition Files*. For details about the setting procedure, see *1.19.6 Specifying settings for handling JP1/IM - Manager failures (for Windows)*, and *2.18.10 Specifying settings for handling JP1/IM - Manager failures (for UNIX)* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

#9: *Original event* refers to the event that JP1/IM - Manager acquired from JP1/Base.

3.2.2 Details of JP1 events output by JP1/IM - Manager

This section describes the details of JP1 events.

(1) Details of event ID: 0002010

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of Automatic Action Service
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	Source serial number
	Message	`MESSAGE`	`KAVB4400-E The run time of an action for an event exceeded the action delay monitoring time. (Event_ID=`*event-ID*`, SEQNO=`*serial-number-in-event-database*`, Execution Host=`*action-execution-host*`, Action Serial Number=`*action-serial-number*`) Delay monitoring notifications will not`

Attribute type		Item	Attribute name	Description
				be sent until suppression of the function for sending notifications to the action delay monitor is canceled.
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		User name	USER_NAME	JP1 user who executed the action
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status
		Command	EXECCMD	Command whose execution was requested
		Environment variable file	EXECENV	Name of the environment variable file used during execution
		Action serial number	ACTION_SEQNO	Serial number of the action
		ID of the action triggering event	SRC_EVENT_ID	Event ID of the event that resulted in execution of the action
		Inserted time	SEND_TIME	Time the action execution request was sent

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(2) Details of event ID: 00002011

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX

Attribute type		Item	Attribute name	Description
				root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4402-E An event status is abnormal.(event ID = *event-ID*, event serial number = *serial-number-in-event-database*, execution host = *action-execution-host*, action serial number = *action-serial-number*) Status monitoring notifications will not be sent until suppression of the function for sending notifications to the action status monitor is canceled
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		User name	USER_NAME	JP1 user who executed the action
		End time	END_TIME	Time the action terminated abnormally
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action's status
		Command	EXECCMD	Command whose execution was requested
		Environment variable file	EXECENV	Name of the environment variable file used during execution
		Action serial number	ACTION_SEQNO	Serial number of the action
		ID of the action triggering event	SRC_EVENT_ID	Event ID of the event that resulted in execution of the action

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(3) Details of event ID: 00002012

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0

Attribute type		Item	Attribute name	Description
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB8060-E An abnormality was detected in` *function-name*`. (host name =` *host-name*`, process name =` *process-name*`, process ID =` *process-ID*`) :` *maintenance-information*
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/HEALTHCHECK`
		Object type	`OBJECT_TYPE`	`JCOHC`
		Object name	`OBJECT_NAME`	Name of the function in which the error was detected
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Host	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Process ID	`PROCESS_ID`	Process ID

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(4) Details of event ID: 00002013

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

Attribute type		Item	Attribute name	Description

		Source user name	`USERNAME`	- In Windows
				`SYSTEM`
				- In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB8062-E An abnormality was detected in` *function-name*`. (host name =` *host-name*`, process name =` *process-name*`) :` *maintenance-information*
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/HEALTHCHECK`
		Object type	`OBJECT_TYPE`	`JCOHC`
		Object name	`OBJECT_NAME`	Name of the function in which the error was detected
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Host	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Process ID	`PROCESS_ID`	Process ID

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(5) Details of event ID: 00002014

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535#1
	Source group ID	`GROUPID`	From -1 to 65,535#1

	Source user name	`USERNAME`	- In Windows
			`SYSTEM`
			- In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank

Attribute type		Item	Attribute name	Description
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB8061-I` *function-name* `has been recovered. (host name =` *host-name*`, process name =` *process-name*`, process ID =` *process-ID*`) :` *maintenance-information*#2
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/HEALTHCHECK`
		Object type	`OBJECT_TYPE`	`JCOHC`
		Object name	`OBJECT_NAME`	Name of the recovered function
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Host	`HOST_NAME`	Host name
		Process name	`PROCESS_NAME`	Process name
		Process ID	`PROCESS_ID`	Process ID

Legend:

--: None

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: If recovery of JP1/Base Event Service (`jevservice`) is detected, the following message is issued: `KAVB8063-I` *function-name* `has been recovered. (host name =` *host-name*`, process name =` *process-name*`) :` *maintenance-information*.

(6) Details of event ID: 00002015

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535#
	Source group ID	`GROUPID`	From -1 to 65,535#

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	Source serial number

Attribute type		Item	Attribute name	Description
		Message	MESSAGE	KAVB4401-I Suppression of the function for sending notifications to the action delay monitor was canceled.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Occurrence	OCCURRENCE	NOTICE

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(7) Details of event ID: 00002016

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4403-I Suppression of the function for sending notifications to the action status monitor was canceled.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Occurrence	OCCURRENCE	NOTICE

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(8) Details of event ID: 00002020

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	Process ID of Automatic Action Service
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4404-E Although the run time of an action exceeded the action delay monitoring time, an action delay notification event could not be sent because no action information exists in the action information file.(action serial number =` *action-serial-number*`) Delay monitoring notifications will not be sent until suppression of the function for sending notifications to the action delay monitor is canceled.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`JCAMAIN`

Attribute type		Item	Attribute name	Description
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action serial number	ACTION_SEQNO	Serial number of the action

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(9) Details of event ID: 00002021

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	Process ID of Automatic Action Service
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4405-E Although an action status is abnormal, an action state notification event could not be sent because no action information exists in the action information file. Status monitoring notifications will not be sent until suppression of the function for sending notifications to the action status monitor is canceled.: *maintenance-information*
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION

Attribute type		Item	Attribute name	Description
		Object name	OBJECT_NAME	JCAMAIN
		User name	USER_NAME	JP1 user who executed the action
		End time	END_TIME	Time the action terminated abnormally
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Serial number of the action
		Action status	ACTION_STATUS	Action's status
		Command	EXECCMD	Command whose execution was requested
		Environment-variable file name	EXECENV	Name of the environment variable file used during execution

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(10) Details of event ID: 000020A0

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows Blank • In UNIX root
	Event-issuing server name	SOURCESERVER	Name of the event-issuing server
	Source serial number	SOURCESEQNO	Source serial number
	Message	MESSAGE	KAVB4054-E Automatic Action was terminated abnormally. (Hostname : *host-name*)

Attribute type		Item	Attribute name	Description
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Occurrence	`OCCURRENCE`	`TERMINATE`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(11) Details of event ID: 000020A1

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	Process ID of Automatic Action Service
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action started
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4050-I Automatic Action was started. :` *logical-host-name*
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Occurrence	`OCCURRENCE`	`START`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(12) Details of event ID: 000020A2

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	Process ID of Automatic Action Service
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535[#] • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535[#] • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action was running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4051-I Automatic Action was terminated. :` *logical-host-name*
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Occurrence	`OCCURRENCE`	`TERMINATE`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(13) Details of event ID: 000020A3

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`

Attribute type		Item	Attribute name	Description
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#1
		Source group ID	GROUPID	From -1 to 65,535#1
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4055-I The action definition file was read and the automatic action function status was changed to operating. The processing will be based on the definitions read from the subsequently received (*arrival-time-of-most-recently-processed-event* (*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*)) events. (Definition=*total-number-of-effective-definitions*/*total-number-of-definitions-in-file*, SEQNO=*serial-number-of-most-recently-processed-event*) #2
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	RUN

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

#2: If the automated action has not received the event, -- is displayed for *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* and for *serial-number-of-last-event-processed*.

(14) Details of event ID: 000020A4

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	From -1 to 65,535#1

Attribute type		Item	Attribute name	Description
		Source group ID	GROUPID	From -1 to 65,535[#1]
		Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4056-I Automatic action was suspended. Automatic actions cannot be executed for the subsequently received (*arrival-time-of-most-recently-processed-event* (*YYYY*/*MM*/*DD* *hh*:*mm*:*ss*)) events. (SEQNO=*serial-number-of-most-recently-processed-event*) [#2]
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	STANDBY

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: If the automated action has not received an event, `--` is displayed for *YYYY*/*MM*/*DD* *hh*:*mm*:*ss* and for *serial-number-of-last-event-processed*.

(15) Details of event ID: 000020A5

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	Process ID of Automatic Action Service
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	- In Windows From -1 to 65,535[#] - In UNIX 0
		Source group ID	GROUPID	- In Windows From -1 to 65,535[#] - In UNIX 0
		Source user name	USERNAME	- In Windows SYSTEM

Attribute type		Item	Attribute name	Description
				• In UNIX `root`
		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the erroneous automated action process was running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4909-E An attempt to set locale information has failed.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Occurrence	`OCCURRENCE`	`ERROR`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(16) Details of event ID: 000020A6

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of Event Base Service
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`

Attribute type		Item	Attribute name	Description
		Event-issuing server name	SOURCESERVER	Name of the logical host where the erroneous Event Base Service process was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4909-E An attempt to set locale information has failed.
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	ERROR

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(17) Details of event ID: 000020E0

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows Blank • In UNIX root
	Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action is running
	Source serial number	SOURCESEQNO	Source serial number
	Message	MESSAGE	KAVB4430-I Execution of the action for an event was requested.

Attribute type		Item	Attribute name	Description
				(Event_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		User name	USER_NAME	JP1 user who executed the action
		Start time	START_TIME	Time the action execution request was completed
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status RUNNING
		Command	EXECCMD	Command whose execution was requested
		Environment-variable file name	EXECENV	Name of the environment variable file used during execution

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(18) Details of event ID: 000020E1

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows Blank

Attribute type		Item	Attribute name	Description
				- In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action was running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4431-I Execution of the action for an event ended normally. (EVENT_ID=`*event-ID*`, SEQNO=`*serial-number-in-event-database*`, Return_code=`*termination-code*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Object ID	`OBJECT_ID`	Serial number of the event that caused the action
		User name	`USER_NAME`	JP1 user who executed the action
		End time	`END_TIME`	Time the action execution request was completed
		Termination code	`RESULT_CODE`	Action's termination code
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Action execution host	`EXECHOST`	Name of the host executing the action
		Action status	`ACTION_STATUS`	Action status `ENDED`
		Command	`EXECCMD`	Command whose execution was requested
		Environment-variable file name	`EXECENV`	Name of the environment variable file used during execution

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(19) Details of event ID: 000020E2

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of Automatic Action Service
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	- In Windows From -1 to 65,535# - In UNIX 0

Attribute type		Item	Attribute name	Description
		Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4432-E Automatic action or command control of the action for an event ended abnormally. (EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		User name	USER_NAME	JP1 user who executed the action
		End time	END_TIME	Time the action terminated abnormally
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status ERROR or FAIL
		Detailed abnormal termination information	ERROR_INFO	Message indicating the nature of the error
		Command	EXECCMD	Command whose execution was requested
		Environment-variable file name	EXECENV	Name of the environment variable file used during execution
		Cause of error	EXECERR	Maintenance information in the event of an error

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(20) Details of event ID: 000020E3

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	Process ID of Automatic Action Service
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4433-I Execution of the action for an action state notification event was requested.(Event_ID=`*event-ID*`, SEQNO=`*serial-number-in-event-database*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Object ID	`OBJECT_ID`	Serial number of the event that caused the action
		User name	`USER_NAME`	JP1 user who executed the action
		Start time	`START_TIME`	Time the action execution request was completed
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Action execution host	`EXECHOST`	Name of the host executing the action
		Action status	`ACTION_STATUS`	Action status `RUNNING`
		Command	`EXECCMD`	Command whose execution was requested

Attribute type		Item	Attribute name	Description
		Environment-variable file name	`EXECENV`	Name of the environment variable file used during execution

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(21) Details of event ID: 000020E4

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	Process ID of Automatic Action Service
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action was running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4434-I Execution of the action for an action state notification event ended normally. (EVENT_ID=`*event-ID*`, SEQNO=`*serial-number-in-event-database*`, Return_code=`*termination-code*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/JCAMAIN`
		Object type	`OBJECT_TYPE`	`ACTION`
		Object name	`OBJECT_NAME`	`JCAMAIN`
		Object ID	`OBJECT_ID`	Serial number of the event that caused the action

Attribute type		Item	Attribute name	Description
		User name	`USER_NAME`	JP1 user who executed the action
		End time	`END_TIME`	Time the action execution request was completed
		Termination code	`RESULT_CODE`	Action's termination code
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Action execution host	`EXECHOST`	Name of the host executing the action
		Action status	`ACTION_STATUS`	Action status `ENDED`
		Command	`EXECCMD`	Command whose execution was requested
		Environment-variable file name	`EXECENV`	Name of the environment variable file used during execution

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(22) Details of event ID: 000020E5

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of Automatic Action Service
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
	Event-issuing server name	`SOURCESERVER`	Name of the logical host where the automated action was running
	Source serial number	`SOURCESEQNO`	Source serial number
	Message	`MESSAGE`	`KAVB4435-E Automatic action or command control of the`

Attribute type		Item	Attribute name	Description
				action for an action state notification event ended abnormally. (EVENT_ID=*event-ID*, SEQNO=*serial-number-in-event-database*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		User name	USER_NAME	JP1 user who executed the action
		End time	END_TIME	Time the action terminated abnormally
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status ERROR or FAIL
		Detailed abnormal termination information	ERROR_INFO	Message indicating the nature of the error
		Command	EXECCMD	Command whose execution was requested
		Environment-variable file name	EXECENV	Name of the environment variable file used during execution
		Cause of error	EXECERR	Maintenance information in the event of an error

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(23) Details of event ID: 000020E6

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
	Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0

Attribute type		Item	Attribute name	Description
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4436-W Although Execution of the action for an event was requested, an action state notification event could not be sent because no action information exists in the action information file. : *maintenance-information*
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		User name	USER_NAME	JP1 user who executed the action
		Start time	START_TIME	Time the action execution request was completed
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status RUNNING
		Command	EXECCMD	Command whose execution was requested
		Environment-variable file name	EXECENV	Name of the environment variable file used during execution

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(24) Details of event ID: 000020E7

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of Automatic Action Service
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time

Attribute type		Item	Attribute name	Description
		Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4437-W Although Execution of the action for an event ended normally, an action state notification event could not be sent because no action information exists in the action information file. : *maintenance-information*
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		End time	END_TIME	Time execution of the action ended
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status ENDED
		Command	EXECCMD	Command whose execution was requested

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(25) Details of event ID: 000020E8

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	Process ID of Automatic Action Service
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the logical host where the automated action was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4438-E Although automatic action or command control of the action for an event ended abnormally, an action state notification event could not be sent because no action information exists in the action information file. : *maintenance-information*
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/JCAMAIN
		Object type	OBJECT_TYPE	ACTION
		Object name	OBJECT_NAME	JCAMAIN
		End time	END_TIME	Time the action terminated abnormally
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action execution host	EXECHOST	Name of the host executing the action
		Action status	ACTION_STATUS	Action status ERROR or FAIL

Attribute type		Item	Attribute name	Description
		Detailed abnormal termination information	ERROR_INFO	Message indicating the nature of the error
		Command	EXECCMD	Command whose execution was requested

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(26) Details of event ID: 00003F01

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	-1
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time of an event that can be acquired
	Source user ID	USERID	0
	Source group ID	GROUPID	0
	Source user name	USERNAME	Blank
	Source group name	GROUPNAME	Blank
	Event-issuing server name	SOURCESERVER	Name of the event-issuing server
	Source serial number	SOURCESEQNO	0
	Message	MESSAGE	KAVB1513-W Cannot display some event(S). There were no events to obtain from the event buffer on the connecting host. All the events except the above will be displayed. To search for an event which was not displayed, specify the search conditions in the event search condition settings dialog as follows: (1) In "Search host", specify the name of the connecting host. (2) In "Registered timeframe", specify the times when the events before and after this event were registered. Check to see if the following conditions are met when this event appears frequently. (1) The "Interval" value that was set for "Automatic refresh" in the Preferences window is too long.

Attribute type		Item	Attribute name	Description
				(2) The "Num. of events to acquire at update" value that was set in the Preferences window is too small. (3) The "Event buffer" value for the Manager that was set in the System Environment Settings window is too small.
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`EVENT`
		Object name	`OBJECT_NAME`	`\SYSTEM\ALL`
		Occurrence	`OCCURRENCE`	`LOST`

(27) Details of event ID: 00003F02

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	`-1`
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Registered time
	Arrived time	`ARRIVEDTIME`	Arrival time of an event that can be acquired
	Source user ID	`USERID`	`0`
	Source group ID	`GROUPID`	`0`
	Source user name	`USERNAME`	Blank
	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	`0`
	Message	`MESSAGE`	KAVB1540-W Cannot display some event(s). (page = *page*) There were no events to obtain from the event buffer on the connecting host. All the events except the above will be displayed. To search for an event which was not displayed, specify the search conditions in the event search condition settings dialog as follows: (1) In "Search host", specify the name of the connecting host.

Attribute type		Item	Attribute name	Description
				(2) In "Registered timeframe", specify the times when the events before and after this event were displayed. Check to see if the following conditions are met when this event appears frequently. (1) The "Interval" value that was set for "Automatic refresh" in the Preferences window is too long. (2) The "Num. of events to acquire at update" value that was set in the Preferences window is too small. (3) The "Event buffer" value for the Manager that was set in the System Environment Settings window is too small.
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`EVENT`
		Object name	`OBJECT_NAME`	`\SYSTEM\ALL`
		Occurrence	`OCCURRENCE`	`LOST`

(28) Details of event ID: 00003F03

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	`-1`
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Time the error occurred
	Source user ID	`USERID`	`0`
	Source group ID	`GROUPID`	`0`
	Source user name	`USERNAME`	Blank
	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	`0`

Attribute type		Item	Attribute name	Description
		Message	MESSAGE	KAVB1516-W An error occurred in acquiring an event from the event service. Cannot recover the error after attempting the number of retries specified in the system profile. No more events will be displayed from now on due to this error. Please check if the event service is running or not. If not, recover the error by re-executing the manager after starting the event service.
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Event Service
		Occurrence	OCCURRENCE	DISCONNECT

(29) Details of event ID: 00003F04

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	-1
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time the error occurred
		Source user ID	USERID	0
		Source group ID	GROUPID	0
		Source user name	USERNAME	Blank
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	0
		Message	MESSAGE	KAVB1527-E A condition that cannot be received by the search host is included.
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Event Service
		Occurrence	OCCURRENCE	PARAM_ERROR

(30) Details of event ID: 00003F05

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	-1
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time the error occurred
		Source user ID	USERID	0
		Source group ID	GROUPID	0
		Source user name	USERNAME	Blank
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	0
		Message	MESSAGE	KAVB0246-E The filter condition exceeds the maximum length. (Maximum length:*maximum-length*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	Event Service
		Occurrence	OCCURRENCE	OVER_LENGTH

(31) Details of event ID: 00003F06

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	-1
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time the error occurred
	Source user ID	USERID	0
	Source group ID	GROUPID	0
	Source user name	USERNAME	Blank
	Source group name	GROUPNAME	Blank
	Event-issuing server name	SOURCESERVER	Name of the event-issuing server
	Source serial number	SOURCESEQNO	0

Attribute type		Item	Attribute name	Description
		Message	`MESSAGE`	`KAVB0248-E The settings for a regular expression is incorrect.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	Event Service or IM database
		Occurrence	`OCCURRENCE`	`REGEXP_ERROR`

(32) Details of event ID: 00003F07

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	`-1`
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Time the error occurred
		Source user ID	`USERID`	`0`
		Source group ID	`GROUPID`	`0`
		Source user name	`USERNAME`	Blank
		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	`0`
		Message	`MESSAGE`	`KAVB4764-W An error occurred in acquiring an event from the event service. Please check if the event service is running or not. If not, recover the error by starting the event service.`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	Event Service
		Occurrence	`OCCURRENCE`	`DISCONNECT`

(33) Details of event ID: 00003F08

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	`-1`
		Source process ID	`PROCESSID`	`0`

Attribute type		Item	Attribute name	Description
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Time the error occurred
		Source user ID	`USERID`	`0`
		Source group ID	`GROUPID`	`0`
		Source user name	`USERNAME`	Blank
		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	`0`
		Message	`MESSAGE`	`KAVB0251-E The search cannot be performed for the specified condition because the search host's JP1/Base does not support the exclusion condition.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	Event Service
		Occurrence	`OCCURRENCE`	`EXCLUDE_ERROR`

(34) Details of event ID: 00003F11

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of occurrence
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535[#1]
	Source group ID	`GROUPID`	From -1 to 65,535[#1]

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	Source serial number

Attribute type		Item	Attribute name	Description
		Message	`MESSAGE`	`KAVB1577-I A status operation was performed. (user who performed the operation =` *JP1-user*#2`, event ID =` *event-ID*`, status before operation =` *status-before-operation*#3`, status after operation =` *status-after-operation*#3`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`PROCESS`
	User-specific or program-specific information	Serial number of the handled event	`PROCESSUPDATE_SEQNO`	Serial number of the JP1 event whose action's status was changed (decimal number)
		Source serial number of the handled event	`PROCESSUPDATE_ORIGINALSEQNO`	Source serial number of the JP1 event whose action's status was changed (decimal number)
		Event level of the handled event	`PROCESSUPDATE_SEVERITY`	Event level of the JP1 event whose action's status was changed (one of the following: `Emergency`, `Alert`, `Critical`, `Error`, `Warning`, `Notice`, `Information`, or `Debug`)
		Source event server name of the handled event	`PROCESSUPDATE_SOURCESERVER`	Name of the event-issuing server (server that issued the JP1 event whose action's status was changed)
		Message for the handled event	`PROCESSUPDATE_MESSAGE`	Message (for the JP1 event whose action's status was changed)
		Registration time of the handled event	`PROCESSUPDATE_TIME`	Time of registration (time the JP1 event whose action's status was changed was registered; displayed in the Event Details window in the format *MM*/*DD* *hh*:*mm*:*ss*)

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: The value that is actually displayed for *JP1-user* depends on the status, as follows:

- When the action status was changed from JP1/IM - View version 08-01 or later: *JP1-user-who-changed-the-action-status*
- When the action status was changed from JP1/IM - View version 07-00 or earlier: `-`
- When the action status was changed by the `jcochstat` command: `jcochstat`
- When the action status was changed because there was a response to a response-waiting event: `system`
- When the action status was changed because a response-waiting event was canceled: `system`

#3: *status-before-action* and *status-after-action* depend on the handling method, as shown below:

- Processed: `PROCESSED`
- Unprocessed: `UNPROCESSED`
- Processing: `PROCESSING`
- Held: `HELD`
- Processed -> Deleted: `PROCESSED+DELETE`
- Unprocessed -> Deleted: `UNPROCESSED+DELETE`
- Processing -> Deleted: `PROCESSING+DELETE`
- Held -> Deleted: `HELD+DELETE`

(35) Details of event ID: 00003F13

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of occurrence
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535[#]
		Source group ID	`GROUPID`	From -1 to 65,535[#]

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the event base server is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4014-I The event acquisition filter definition file was read. The read definitions will be used for processing from the next received event. (filter name =` *filter-name*`, last received event =` *arrival-time*`, serial number in event DB =` *serial-number*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(36) Details of the event ID specified in the SUCCESS_EVENT parameter in the correlation event generation definition file

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`IDBASE`	User-defined event ID (must be in the range from `0` to `1FFF` and from `7FFF8000` to `7FFFFFFF`)
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration

Attribute type		Item	Attribute name	Description
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	User-defined message
Extended attribute	Common information	Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/GENERATE_EVENT`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EGS`
		Occurrence	`OCCURRENCE`	`SUCCESS`
	User-specific or program-specific information	Relation Event serial number	`JP1_GENERATE_SOURCE_SEQNO`	Serial numbers of related events separated by the space (Δ), as shown below: *serial-number-1Δserial-number-2Δ...Δserial-number-n* (*n*: value from 1 to 100)
		Correlation event generation condition name	`JP1_GENERATE_NAME`	Name of the correlation event generation condition that resulted in approval

Note: You can define as correlation event attributes additional attributes that are not listed in this table. For details, see *Correlation event generation definition file* in *Chapter 2. Definition Files*.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(37) Details of the event ID specified in the FAIL_EVENT parameter in the correlation event generation definition file

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`IDBASE`	User-defined event ID (must be in the range from `0` to `1FFF` and from `7FFF8000` to `7FFFFFFF`)
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535#
	Source group ID	`GROUPID`	From -1 to 65,535#

Attribute type		Item	Attribute name	Description

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
Extended attribute	Common information	Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/GENERATE_EVENT`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EGS`
		Occurrence	`OCCURRENCE`	`FAIL`
	User-specific or program-specific information	Relation Event serial number	`JP1_GENERATE_SOURCE_SEQNO`	Serial numbers of related events separated by the space (Δ), as shown below: *serial-number-1*Δ*serial-number-2*Δ...Δ*serial-number-n* (*n*: value from 1 to 100)
		Correlation event generation condition name	`JP1_GENERATE_NAME`	Name of the correlation event generation condition that resulted in failure

Note: You can define as correlation event attributes additional attributes that are not listed in this table. For details, see *Correlation event generation definition file* in *Chapter 2. Definition Files*.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(38) Details of event ID: 00003F15

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`3F15`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of Automatic Action Service
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535[#1] • In UNIX 0
	Source group ID	`GROUPID`	• In Windows From -1 to 65,535[#1] • In UNIX 0
	Source user name	`USERNAME`	• In Windows `SYSTEM` • In UNIX

Attribute type		Item	Attribute name	Description
				`root`
		Source group name	`GROUPNAME`	- In Windows Blank - In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the event base server is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB1669-I The severe event definition file has been read. Next, processing will be performed using the definition read from the acquired event. (Event acquired at the end:Arrival time =` *arrival-time-of-the-event-acquired-at-the-end*`, serial number in event DB =` *serial-number-in-event-database-of-the-event-acquired-at-the-end*`)` #2
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: If Event Base Service has not received the event, `--` is displayed for *arrival-time-of-last-event-acquired* and for *serial-number-of-last-event-acquired*.

(39) Details of event ID: 00003F16

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	`SEQNO`	`-1`
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Time the error occurred
	Source user ID	`USERID`	`0`
	Source group ID	`GROUPID`	`0`
	Source user name	`USERNAME`	Blank
	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
	Source serial number	`SOURCESEQNO`	`0`

Attribute type		Item	Attribute name	Description
		Message	MESSAGE	KAVB1671-W An error occurred in acquiring an event from the integrated monitoring database. Cannot recover the error after attempting the number of retries specified in the system profile. No more events will be displayed from now on due to this error.
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	IM Database
		Occurrence	OCCURRENCE	DISCONNECT

(40) Details of event ID: 00003F17

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the event base server is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB1150-I An additional common exclusion conditions group was registered. (common exclusion conditions group ID = *common-exclusion-conditions-group-ID*, common exclude conditions group name = *common-exclude-conditions-group-name*, registering user = *user-name*)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW

Attribute type		Item	Attribute name	Description
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(41) Details of event ID: 00003F20

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the Event Generation Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAJV2179-I The event acquisition filter definition file was read. The read definitions will be used for processing from the next received event. (filter name = *filter-name*, last received event = *arrival-time*, serial number in event DB = *serial-number-in-event-database*)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EGS
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EGS
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(42) Details of event ID: 00003F21

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the Event Generation Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAJV2242-I The correlation event generation definition file has been read, and the definitions for the correlation event generation function have been updated. (file name = *file-name*)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EGS
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EGS
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(43) Details of event ID: 00003F22

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	From -1 to 65,535#
	Source group ID	GROUPID	From -1 to 65,535#
	Source user name	USERNAME	- In Windows

Attribute type		Item	Attribute name	Description
				SYSTEM - In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the event base server was running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4712-W The event base service cannot use common exclusion condition groups (extended) because a regular expression used by JP1/Base is not extended. The event base service will start without any common exclusion condition groups (extended) being set.
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	Notice

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(44) Details of event ID: 00003F23

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the event base server is running
		Source serial number	SOURCESEQNO	Source serial number

Attribute type		Item	Attribute name	Description
		Message	`MESSAGE`	`KAJV2502-W The correlation event issuing service cannot use common exclusion condition groups (extended) because the regular expressions used by JP1/Base are not extended. The correlation event issuing service will start without any common exclusion condition groups (extended) being set.`
Extended attribute	Common information	Event level	`SEVERITY`	`Notice`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EGS`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EGS`
		Occurrence	`OCCURRENCE`	`Notice`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(45) Details of event ID: 00003F25

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the logical host where the Event Generation Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAJV2243-I The correlation event generation function has been restarted.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EGS`
		Object type	`OBJECT_TYPE`	`SERVICE`

Attribute type		Item	Attribute name	Description
		Object name	OBJECT_NAME	EGS
		Occurrence	OCCURRENCE	START

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(46) Details of event ID: 00003F26

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the logical host where the Event Generation Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAJV2234-I The correlation event generation function has stopped.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EGS
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EGS
		Occurrence	OCCURRENCE	STOP

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(47) Details of event ID: 00003F28

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#

Attribute type		Item	Attribute name	Description
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAJV2322-W A JP1 event (event ID=*event-ID*, serial number in the event database=*serial-number*) could not be correlated because the number of correlated JP1 event pairs has reached the upper limit (20,000).
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EGS
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EGS
		Occurrence	OCCURRENCE	RUN

Note: JP1 event 00003F28 is output once when the number of JP1 event sets reaches the maximum value. After that, this event is not output again until the number of JP1 event sets drops down to 16,000 or fewer.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(48) Details of event ID: 00003F31

Attribute type	Item	Attribute name	Description
Basic attribute	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	From -1 to 65,535#
	Source group ID	GROUPID	From -1 to 65,535#
	Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
	Source group name	GROUPNAME	Blank
	Event-issuing server name	SOURCESERVER	Name of the logical host where the Event Generation Service is running

Attribute type		Item	Attribute name	Description
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAJV2188-I An additional common exclusion conditions group was registered. (common exclusion conditions group ID =` *common-exclusion-conditions-group-ID*, `common exclude conditions group name` = *common-exclude-conditions-group-name*, registering user = *user-name*)
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EGS`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EGS`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(49) Details of event ID: 00003F41

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of occurrence
		Arrived time	`ARRIVEDTIME`	Arrived time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB0551-E The number of accumulated response-waiting events on the manager exceeded the maximum (2000).`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`

Attribute type		Item	Attribute name	Description
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVTCON
		Occurrence	OCCURRENCE	NOTICE

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(50) Details of event ID: 00003F42

Attribute type		Item	Attribute name	Description
Basic attribute		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of occurrence
		Arrived time	ARRIVEDTIME	Arrived time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB1816-W A response-waiting event could not be displayed. To search for the event, specify the search conditions in the dialog box for setting the event search conditions as follows: (1) As the host to be searched for, specify the name of the connected host. (2) As the response-waiting event, specify the target event. (3) As the arrival timeframe, specify the times when the events before and after this event arrived.
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE

Attribute type		Item	Attribute name	Description
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`PROCESS`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(51) Details of event ID: 00003F51

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F51`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#1
		Source group ID	`GROUPID`	From -1 to 65,535#1

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB1841-I The events from` *deletion-target-start-date-and-time* `to` *deletion-target-end-date-and-time* `were deleted from the integrated monitoring database.`#2
Extended attribute	Common information	Event level	`SEVERITY`	`Notice`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Deletion start date	`DEL_STARTDAY`	Deletion start date, expressed as absolute time in seconds (displayed in the Event Details window in the format *MM*`/`*DD* *hh*`:`*mm*`:`*ss*)
		Deletion end date	`DEL_ENDDAY`	Deletion end date, expressed as absolute time in seconds (displayed in the Event Details window in the format *MM*`/`*DD* *hh*`:`*mm*`:`*ss*)

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: The format of *deletion-start-date* and *deletion-end-date* is replaced in the `KAVB1841-I` message with *YYYY*`/`*MM*`/`*DD* *hh*`:`*mm*`:`*ss*.

(52) Details of event ID: 00003F52

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	ID	00003F52
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB1842-W Events not output for preservation have exceeded the deletion warning level (*deletion-warning-level*%).
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	NOTICE

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(53) Details of event ID: 00003F53

Attribute type		Item	Attribute name	Description
Basic attribute		Source host	SOURCESERVER	Name of the event-issuing server
		Message	MESSAGE	KAVB1832-E An error occur while attempting to register an event into the integrated monitoring database. The system will retry registering the event. (detailed information = *detailed-information*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW

Attribute type		Item	Attribute name	Description
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`NOTICE`

(54) Details of event ID: 00003F54

Attribute type		Item	Attribute name	Description
Basic attribute		Source host	`SOURCESERVER`	Name of the event-issuing server
		Message	`MESSAGE`	`KAVB1833-I An error occur while attempting to register an event into the integrated monitoring database. However, after several retries, the event was registered into the database. The event base service is restarting event acquisition.`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`NOTICE`

(55) Details of event ID: 00003F56

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	00003F56
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrived time
	Source user ID	`USERID`	From -1 to 65,535#
	Source group ID	`GROUPID`	From -1 to 65,535#

	Source user name	`USERNAME`	- In Windows
			`SYSTEM`
			- In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the logical host where the event base server is running
	Source serial number	`SOURCESEQNO`	Source serial number
	Message	`MESSAGE`	`KAVB4673-I A repeated event condition was registered. (repeated`

Attribute type		Item	Attribute name	Description
				`event condition name = `*repeated-event-condition-name*`, registering user = `*user-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(56) Details of event ID: 00003F57

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F57`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrived time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	- In Windows
				`SYSTEM`
				- In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the host or the logical host where the event base server is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4674-I The definition file for the repeated event condition was updated. Next, processing will be performed using the definition read from the received event. (arrival time of the last received event = `*arrival-time-of-the-last-received-event*`, serial number in the event database = `*serial-number-in-the-event-database*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`

Attribute type		Item	Attribute name	Description
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(57) Details of event ID: 00003F58

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	ID	00003F58
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Arrived time
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the host or the logical host where the event base server is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4676-I Suppression of repeated events that match the repeated event condition (*repeated-event-condition-name*) has started. (arrival time of the first suppressed event = *arrival-time-of-the-first-suppressed-event*, event database serial number of the first suppressed event = *event-database-serial-number-of-the-first-suppressed-event*)
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	NOTICE

Attribute type		Item	Attribute name	Description
	User-specific or program-specific information	Duplicate attribute value information 1	`SAMEATTR1`	Stores the first (listed at the top) attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If a duplicate attribute value condition is not specified, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 2	`SAMEATTR2`	Stores the second attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there are fewer than two duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 3	`SAMEATTR3`	Stores the third attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there are fewer than three duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(58) Details of event ID: 00003F59

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`00003F59`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrived time
	Source user ID	`USERID`	From -1 to 65,535#
	Source group ID	`GROUPID`	From -1 to 65,535#

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the host or the logical host where the event base server is running

Attribute type		Item	Attribute name	Description
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4677-I Suppression of repeated events that match the repeated event condition (*repeated-event-condition-name*) has ended. (arrival time of the suppressed event = *arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* - *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*, event database serial number of the suppressed event = *event-database-serial-number-of-the-first-suppressed-event* - *event-database-serial-number-of-the-last-suppressed-event*)
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Duplicate attribute value information 1	SAMEATTR1	Stores the first (listed at the top) attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If a duplicate attribute value condition is not specified, a blank is stored. You can specify maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 2	SAMEATTR2	Stores the second attribute name and its value as a duplicate attribute value conditions in *attribute-name=attribute-value* format. If there are fewer than two duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 3	SAMEATTR3	Stores the third attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there are fewer than three duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(59) Details of event ID: 00003F60

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F60`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Registered time
		Arrived time	`ARRIVEDTIME`	Arrived time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the host or the logical host where the event base server is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4678-I Suppression of repeated events that match the repeated event condition (`*repeated-event-condition-name*`) has terminated. (arrival time of the suppressed event =` *arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* `-` *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*`, event database serial number of the suppressed event =` *event-database-serial-number-of-the-first-suppressed-event* `-` *event-database-serial-number-of-the-last-suppressed-event*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Notice`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Duplicate attribute value information 1	`SAMEATTR1`	Stores the first (listed at the top) attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If a duplicate attribute value condition is not specified, a blank is stored.

Attribute type		Item	Attribute name	Description
				You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 2	`SAMEATTR2`	Stores the second attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there is only one duplicate attribute value condition, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 3	`SAMEATTR3`	Stores the third attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there are fewer than three duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(60) Details of event ID: 00003F61

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`00003F61`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535[#1]
	Source group ID	`GROUPID`	From -1 to 65,535[#1]

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where Event Base Service is running
	Source serial number	`SOURCESEQNO`	Source serial number
	Message	`MESSAGE`	`KAVB4600-I The severity change definition has been read. Next,`

Attribute type		Item	Attribute name	Description
				processing will be performed using the definition read from the received event. (arrival time of the last received event = *arrival-time*, serial number in the event database = *serial-number-in-event-database*)[#2]
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	RUN

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

#2: The format of *arrival-time* is replaced in the KAVB4600-I message with *YYYY*/*MM*/*DD* *hh*:*mm*:*ss*. The time set in *arrival-time* is based on the time zone set in the machine where JP1/IM - Manager is running.

(61) Details of event ID: 00003F63

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	ID	00003F63
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Arrival time
	Source user ID	USERID	From -1 to 65,535[#1]
	Source group ID	GROUPID	From -1 to 65,535[#1]
	Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
	Source group name	GROUPNAME	Blank
	Event-issuing server name	SOURCESERVER	Name of the server or logical host where the Event Base Service is running
	Source serial number	SOURCESEQNO	Source serial number
	Message	MESSAGE	KAVB4650-I An event-source-host mapping definition was read. Processing will be performed by the definition read from the next received event. (last received event: reception time = *reception-time*, event database serial number = *event-database-serial-number*)[#2]

Attribute type		Item	Attribute name	Description
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: The format of *arrival-time* is replaced in the `KAVB4650-I` message with *YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*. The time set in *arrival-time* is based on the time zone set in the machine where JP1/IM - Manager is running.

(62) Details of event ID: 00003F64

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F64`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#1
		Source group ID	`GROUPID`	From -1 to 65,535#1

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the host or logical host where the Event Base Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB8453-I The business group was updated. Processing will be performed from the next-received event. (last received event: reception time =` *reception-time*`, event database serial number =` *event-database-serial-number*`)`#2
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: The format of *arrival-time* is replaced in the KAVB8453-I message with *YYYY*/*MM*/*DD hh*:*mm*:*ss*. The time set in *arrival-time* is based on the time zone set in the machine where JP1/IM - Manager is running.

(63) Details of event ID: 00003F65

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	ID	00003F65
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Registered time
		Arrived time	ARRIVEDTIME	Arrived time
		Source user ID	USERID	-1 to 65,535#
		Source group ID	GROUPID	-1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the host or logical host where the Event Base Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4679-I Suppression of repeated events that match the repeated event condition (*repeated-event-condition-name*) will continue. (arrival time of the suppressed event = *arrival-time-of-the-first-suppressed-event(YYYY/MM/DD HH:MM:SS)* - *arrival-time-of-the-last-suppressed-event(YYYY/MM/DD HH:MM:SS)*, event database serial number of the suppressed event = *event-database-serial-number-of-the-first-suppressed-event* - *event-database-serial-number-of-the-last-suppressed-event*)
Extended attribute	Common information	Event level	SEVERITY	Notice
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Duplicate attribute value information 1	SAMEATTR1	Stores the first (listed at the top) attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format.

Attribute type		Item	Attribute name	Description
				If a duplicate attribute value condition is not specified, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 2	`SAMEATTR2`	Stores the second attribute name and its value as a duplicate attribute value conditions in *attribute-name=attribute-value* format. If there are fewer than two duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.
		Duplicate attribute value information 3	`SAMEATTR3`	Stores the third attribute name and its value as a duplicate attribute value condition in *attribute-name=attribute-value* format. If there are fewer than three duplicate attribute value conditions, a blank is stored. You can specify a maximum of 1,024 bytes for the attribute value. For a value larger than 1,024 bytes, split it, but do so without splitting a multi-byte character.

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(64) Details of event ID: 00003F68

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`00003F68`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From -1 to 65,535#
	Source group ID	`GROUPID`	From -1 to 65,535#

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank
	Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where the Event Base Service is running
	Source serial number	`SOURCESEQNO`	Source serial number

Attribute type		Item	Attribute name	Description
		Message	`MESSAGE`	`KAVB8454-W The business group could not be updated. (cause =` *cause*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(65) Details of event ID: 00003F69

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F69`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Time of registration
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From -1 to 65,535#
		Source group ID	`GROUPID`	From -1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where Event Base Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB8456-E The business group could not be updated. (cause =` *cause*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(66) Details of event ID: 00003F6A

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F6A`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Registered time
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From `-1` to `65535`[#1]
		Source group ID	`GROUPID`	From `-1` to `65535`[#1]

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where Event Base Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4623-I The display message change definition has been read. Next, processing will be performed using the definition read from the received event. (arrival time of the last received event =` *arrival-time*`, serial number in the event database =` *event-database-serial-number*`)` [#2]
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVFLOW`
		Occurrence	`OCCURRENCE`	`RUN`

#1: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

#2: The format of *arrival-time* is replaced in the `KAVB4623-I` message with *YYYY*`/`*MM*`/`*DD hh*`:`*mm*`:`*ss*. The time set in *arrival-time* is based on the time zone set in the machine where JP1/IM - Manager is running.

(67) Details of event ID: 00003F71

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`00003F71`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`

Attribute type		Item	Attribute name	Description
		Registered time	`TIME`	Registered time
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	-1 to 65,535#
		Source group ID	`GROUPID`	-1 to 65,535#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where Event Base Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB4802-I A severity change definition was registered. (severity change definition name =` *severity-change-definition-name*`, registering user =` *user-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVFLOW`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(68) Details of event ID: 00003F76

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	`ID`	`00003F76`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Registered time
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	From `-1` to `65535`#
	Source group ID	`GROUPID`	From `-1` to `65535`#

	Source user name	`USERNAME`	• In Windows
			`SYSTEM`
			• In UNIX
			`root`

	Source group name	`GROUPNAME`	Blank

Attribute type		Item	Attribute name	Description
		Event-issuing server name	SOURCESERVER	Name of the server or logical host where Event Base Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB4803-I A display message change definition was registered. (display message change definition name = *display-message-change-definition-name*, registering user = *user-name*)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVFLOW
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVFLOW
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(69) Details of event ID: 00003F77

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	ID	00003F77
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Registered time
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65535#
		Source group ID	GROUPID	From -1 to 65535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the server or logical host where Event Console Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB5800-I The definition file for extended event attributes was read in to JP1/IM - Manager.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE

Attribute type		Item	Attribute name	Description
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(70) Details of event ID: 00003F78

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	`ID`	`00003F78`
		Serial number	`SEQNO`	Serial number
		Source process ID	`PROCESSID`	`0`
		Registered time	`TIME`	Registered time
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	From `-1` to `65535`#
		Source group ID	`GROUPID`	From `-1` to `65535`#

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	Blank
		Event-issuing server name	`SOURCESERVER`	Name of the server or logical host where Event Console Service is running
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB5804-E An attempt to read the definition file for extended event attributes failed because part of the definition file for extended event attributes could not be read.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/EVENTCONSOLE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`EVTCON`
		Occurrence	`OCCURRENCE`	`RUN`

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(71) Details of event ID: 00003F7C

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	ID	00003F7C
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Registered time
		Arrived time	ARRIVEDTIME	Arrival time
		Source user ID	USERID	From -1 to 65535#
		Source group ID	GROUPID	From -1 to 65535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	Blank
		Event-issuing server name	SOURCESERVER	Name of the server or logical host where Event Console Service is running
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB1981-I The definition file for opening monitor windows was applied to JP1/IM - Manager.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/EVENTCONSOLE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	EVTCON
		Occurrence	OCCURRENCE	RUN

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(72) Details of event ID: 00003FB0

Attribute type		Item	Attribute name	Description
Basic attribute		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Message	MESSAGE	KAVB7900-I Status of *monitoring-node-name* is changed *status* from *status*.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/SCOPE
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	IM_CS
		Occurrence	OCCURRENCE	STATUS_CHANGE

Attribute type		Item	Attribute name	Description
	User-specific or program-specific information	Monitoring node ID	`MON_NODE_ID`	ID of the monitoring node
		Monitoring node name	`MON_NODE_NAME`	Name of the monitoring node
		Monitoring node status#1	`MON_NODE_STATUS`	`StatusID` of the monitoring node
		Information about the JP1 event resulting in the status change#2	*attributes*	Attributes (the name of a basic attribute is prefixed with `JCS_B_`, and the name of an extended attribute is prefixed with `JCS_E_`)

#1: For the monitoring node status (`E.MON_NODE_STATUS`), the status of the monitoring node that issued the JP1 event is stored in `StatusID`, expressed as a numeric value as shown below:

Value of `StatusID` (monitoring node status):

`Emergency`: `800`; `Alert`: `700`; `Critical`: `600`; `Error`: `500`; `Warning`: `400`; `Normal`: `300`; `Debug`: `200`; `Initial`: `100`

For example, if a JP1 event is issued when the monitoring node status has changed to `Emergency`, its monitoring node status (`E.MON_NODE_STATUS`) would be `800`.

#2: The item *Information about the JP1 event resulting in the status change* cannot be checked by JP1/IM - View. All information about the JP1 event resulting in the status change is stored in this item as sets of *attribute-name*–*attribute-value*. If `00003FB0` exceeds the maximum length for a JP1 event (10,000 bytes), JP1/IM stores as much JP1 event information as fits. If the number of extended attributes exceeds 100, JP1/IM stores as much JP1 event information as fits, but no more than 100 extended attributes. The attributes `E.JCS_B_TIME` (registration time of the JP1 event resulting in the status change) and `E.JCS_B_ARRIVEDTIME` (arrival time of the JP1 event resulting in the status change) are stored in this item in GMT in the format *YYYY*`/`*MM*`/`*DD* *hh*`:`*mm*`:`*ss*.

(73) Details of event ID: 00003FB1

Attribute type		Item	Attribute name	Description
Basic attribute		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Event ID	--	`00003FB1`
		Message	`MESSAGE`	`KAVB7901-W The number of status change event for the monitored node` *monitoring-node-ID*# `has reached the threshold.`
Extended attribute	Common information	Event level	`SEVERITY`	`WARNING`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/SCOPE`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`IM_CS`
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitoring node ID	`MON_NODE_ID`	ID of the monitoring node
		Number of status change events	`EVHIST_NUMBER`	Number of status change events

Legend:

--: None

#: Only one JP1 event with event ID `00003FB1` is issued even if a single JP1 event triggered more than 100 status change events from multiple monitoring objects. A maximum of 10 monitoring object IDs can be listed in *monitoring-node-ID* in the message, separated by the comma. If there are more than 10 monitoring object IDs, `...` is displayed following the last listed ID.

(74) Details of event ID: 00003FC0

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC0
		Message	MESSAGE	KNAN26102-E The remote log-file trap cannot start. (Code: *code*, Host name: *host name*, Monitoring-target-name: *monitoring-target-name*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	In Windows: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP In UNIX: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/REMOTE_UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitoring name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitoring name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitoring stop time	WATCH_STOP_TIME	Time that log file monitoring stopped (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(75) Details of event ID: 00003FC1

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC1
		Message	`MESSAGE`	`KNAN26094-E The relevant log file could not be read after the specified number of retires, so monitoring will stop. (Code:` *code*, `Host name:` *host-name*, `Monitoring-target-name:` *monitoring-target-name*, `Log file name:` *Log file name*)
Extended attribute	Common information	Event level	`SEVERITY`	`Error`

		Product name	`PRODUCT_NAME`	In Windows:
				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*,
				where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*,
				where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitoring name

Attribute type		Item	Attribute name	Description
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitoring stop time	`WATCH_STOP_TIME`	Time that log file monitoring stopped (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(76) Details of event ID: 00003FC2

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC2
		Message	`MESSAGE`	`KNAN26095-E The relevant log file can no longer be monitored. (Code:` *code*, `Host name:` *host-name*, `Monitoring-target-name:` *monitoring-target-name*, `Log file name:` *Log file name*)
Extended attribute	Common information	Event level	`SEVERITY`	`Error`

		Product name	`PRODUCT_NAME`	In Windows:
				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`

Attribute type		Item	Attribute name	Description
		Object name	OBJECT_NAME	Monitoring name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitoring name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Time an abnormality detected	WATCH_CHECK_TIME	Time that a log file error was detected (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(77) Details of event ID: 00003FC3

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC3
		Message	MESSAGE	KNAN26057-E The remote log-file trap will stop due to error. (Code: *code*, Host name: *host name*, Monitoring-target-name: *monitoring-target-name*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	In Windows: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP In UNIX: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified:

Attribute type		Item	Attribute name	Description
				/HITACHI/JP1/IM/ REMOTE_UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitoring name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitoring name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Time an abnormality detected	WATCH_CHECK_TIME	Time that a log file error was detected (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(78) Details of event ID: 00003FC5

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC5
		Message	MESSAGE	KNAN26140-W The amount of data that a remote log file trap collected from the log file exceeded the limit. The log entries output from the last collection time to this collection time will not be output as JP1 events. (host name: *host name*, monitoring-target name: *monitoring-target-name*, log file name: *Log file name*, previous collection time: *Last collection time*(*yyyy/MM/dd hh:mm:ss*), this collection time: *This collection time*(*yyyy/MM/dd hh:mm:ss*))
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	In Windows: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/ REMOTE_NT_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified:

Attribute type		Item	Attribute name	Description
				/HITACHI/JP1/IM/ REMOTE_NT_LOGTRAP In UNIX: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/ REMOTE_UX_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/ REMOTE_UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitoring name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitoring name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(79) Details of event ID: 00003FC6

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC6
		Message	MESSAGE	KNAN26351-E All trapping of remote log files on monitored host "*monitored-host-name*" will now stop. (cause = *cause*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	In Windows: /HITACHI/JP1/IM/ REMOTE_NT_LOGTRAP In UNIX: /HITACHI/JP1/IM/ REMOTE_UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitored host name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE

Attribute type		Item	Attribute name	Description
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitoring stop time	WATCH_STOP_TIME	Time that log file monitoring stopped (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(80) Details of event ID: 00003FC7

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC7
		Message	MESSAGE	KNAN26350-W The backup files for the monitored log files were not found. The log entries output to the backup files between the previous collection time and the current collection time will not be output as JP1 events. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*, log file name = *monitored-log-file-name*, previous collection time = *yyyy*/*MM*/*dd hh*:*mm*:*ss*, current collection time = *yyyy*/*MM*/*dd hh*:*mm*:*ss*, user = *user*, command line that was executed = *command-line-executed*)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	In Windows: When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/REMOTE_NT_LOGTRAP In UNIX:

Attribute type		Item	Attribute name	Description
				When the -p option of the jcfallogstart command is specified: /HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option of the jevlogstart command. When the -p option of the jcfallogstart command is not specified: /HITACHI/JP1/IM/REMOTE_UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitoring target name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(81) Details of event ID: 00003FC8

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FC8
		Message	MESSAGE	KNAN26352-W The backup files for the monitored log files were not found. The log entries output to the backup files between the previous collection time and the current collection time will not be output as JP1 events. (host name = *monitored-host-name*, monitoring target = *monitoring-target-name*, log file name = *monitored-log-file-name*, last collection time = *yyyy*/*MM*/*dd* *hh*:*mm*:*ss*, current collection time = *yyyy*/*MM*/*dd* *hh*:*mm*:*ss*, user = *user*)
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	In Windows:

Attribute type		Item	Attribute name	Description

				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				When the `-p` option of the `jcfallogstart` command is specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the log data output source program name specified by the `-p` option of the `jevlogstart` command.
				When the `-p` option of the `jcfallogstart` command is not specified:
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring target name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(82) Details of event ID: 00003FC9

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	`00003FC9`
	Message	`MESSAGE`	`KNAN26353-E Trapping of remote event log files on monitored host "`*monitored-host-name*`" will now stop. (cause = `*cause*`)`

Attribute type		Item	Attribute name	Description
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/ REMOTE_NTEVENT_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitored host name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitoring stop time	WATCH_STOP_TIME	Time that log file monitoring stopped (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(83) Details of event ID: 00003FD0

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD0
		Message	MESSAGE	KNAN26107-E The remote event-log trap cannot start. (Code: *code*, Host name: *host name*)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/ REMOTE_NTEVENT_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitored host name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Error detection time	ERROR_TIME	Time that the error occurred (absolute time in seconds since UTC 1970-01-01 00:00:00)
		API where error occurred	ERROR_FUNCTION	Name of the Windows API where the error occurred
		Cause of error	ERROR_CAUSE_ID	Error cause code
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(84) Details of event ID: 00003FD1

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD1
		Message	`MESSAGE`	`KNAN26028-E Monitoring will now stop because the event log could not be read after the specified number of retries. (Code:` *code*`, Host name:` *host name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Error detection time	`ERROR_TIME`	Time that the error occurred (absolute time in seconds since UTC 1970-01-01 00:00:00)
		API where error occurred	`ERROR_FUNCTION`	Name of the Windows API where the error occurred
		Cause of error	`ERROR_CAUSE_ID`	Error cause code
		Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(85) Details of event ID: 00003FD2

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD2
		Message	`MESSAGE`	`KNAN26027-I The system will now retry reading the event log. (Code:` *code*`, Host name:` *host name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`

Attribute type		Item	Attribute name	Description
	User-specific or program-specific information	Error detection time	`ERROR_TIME`	Time that the error occurred (absolute time in seconds since UTC 1970-01-01 00:00:00)
		API where error occurred	`ERROR_FUNCTION`	Name of the Windows API where the error occurred
		Cause of error	`ERROR_CAUSE_ID`	Error cause code
		Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(86) Details of event ID: 00003FD3

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD3
		Message	`MESSAGE`	`KNAN26002-E The remote event-log trap will now stop due to error. (Code:` *code*`, Host name:` *host name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Error detection time	`ERROR_TIME`	Time that the error occurred (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Cause of error	`ERROR_CAUSE_ID`	Error cause code
		Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(87) Details of event ID: 00003FD4

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD4
		Message	`MESSAGE`	`KNAN26026-I An event log can now be monitored. (Host name:` *host name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`

Attribute type		Item	Attribute name	Description
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitored host name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Error detection time	ERROR_TIME	Time that the error occurred (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Error recovery time	RECOVER_TIME	Time that the program was recovered after the error (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Cause of error	ERROR_CAUSE_ID	Error cause code
		Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(88) Details of event ID: 00003FD5

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	00003FD5
		Message	MESSAGE	KNAN26142-W The amount of data that a remote event-log trap collected from the host exceeded the limit. The event-log entries output from the last collection time to this collection time will not be output as JP1 events. (host name = *host name*,previous collection time = *Last collection time*(*yyyy/MM/dd hh:mm:ss*),this collection time = *This collection time*(*yyyy/MM/dd hh:mm:ss*))
Extended attribute	Common information	Event level	SEVERITY	Warning
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Monitored host name
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE

Attribute type		Item	Attribute name	Description
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(89) Details of event ID: 00003FD6

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FD6`
		Message	`MESSAGE`	`KNAN26339-W Failed to save the state of the remote log file trap when the log was collected. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`

		Product name	`PRODUCT_NAME`	In Windows:
				(When the `-p` option of the `jcfallogstart` command is specified)
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command
				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				(When the `-p` option of the `jcfallogstart` command is specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command
				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring target name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`

Attribute type		Item	Attribute name	Description
		Root object name	`ROOT_OBJECT_NAME`	Monitoring target name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(90) Details of event ID: 00003FD7

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FD7`
		Message	`MESSAGE`	`KNAN26340-W Failed to save the state of the remote event log trap when the log was collected. (host name =` *monitored-host-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(91) Details of event ID: 00003FD8

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FD8`
		Message	`MESSAGE`	`KNAN26341-W Failed to restore the remote log file trap to its state when it was last terminated. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	In Windows:

Attribute type		Item	Attribute name	Description

				(When the `-p` option of the `jcfallogstart` command is specified)
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command
				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				(When the `-p` option of the `jcfallogstart` command is specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command
				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring target name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitoring target name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(92) Details of event ID: 00003FD9

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	`00003FD9`
	Message	`MESSAGE`	`KNAN26342-W Failed to restore the remote log file trap to its state when it was last terminated. (host name =` *monitored-host-name*`)`

Attribute type		Item	Attribute name	Description
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitored host name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(93) Details of event ID: 00003FDA

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FDA`
		Message	`MESSAGE`	`KNAN26343-W The remote log file trap was not restored to its state when it was last terminated, because the trap was in a state where it could not be monitored. (details =` *detailed-information*`, host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`, log file name =` *log-file-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	In Windows: (When the `-p` option of the `jcfallogstart` command is specified) `/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command (When the `-p` option of the `jcfallogstart` command is not specified) `/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP` In UNIX:

Attribute type		Item	Attribute name	Description
				(When the `-p` option of the `jcfallogstart` command is specified) `/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command (When the `-p` option of the `jcfallogstart` command is not specified) `/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring target name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitoring target name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(94) Details of event ID: 00003FDB

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FDB`
		Message	`MESSAGE`	`KNAN26345-I An error in the processing to save the state of the remote log file trap that occurred during log collection was resolved. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	In Windows: (When the `-p` option of the `jcfallogstart` command is specified) `/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP/`*program-name*, where *program-name* is the name of the program that output the log data and that is specified for the `-p` option of the `jevlogstart` command

Attribute type		Item	Attribute name	Description

				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_NT_LOGTRAP`
				In UNIX:
				(When the `-p` option of the `jcfallogstart` command is specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP/`*program-name*, where *program-name* is the name of the program name that output the log data and that is specified for the `-p` option of the `jevlogstart` command
				(When the `-p` option of the `jcfallogstart` command is not specified)
				`/HITACHI/JP1/IM/REMOTE_UX_LOGTRAP`

		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitoring target name
		Root object type	`ROOT_OBJECT_TYPE`	`LOGFILE`
		Root object name	`ROOT_OBJECT_NAME`	Monitoring target name
		Occurrence	`OCCURRENCE`	`NOTICE`
	User-specific or program-specific information	Monitored host name	`JP1_SOURCEHOST`	Monitored host name

Legend:

--: None

(95) Details of event ID: 00003FDC

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	`00003FDC`
		Message	`MESSAGE`	`KNAN26346-I An error in the processing to save the state of the remote event log trap that occurred during log collection was resolved. (host name =` *monitored-host-name*`, monitoring target =` *monitoring-target-name*`)`
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/REMOTE_NTEVENT_LOGTRAP`
		Object type	`OBJECT_TYPE`	`LOGFILE`
		Object name	`OBJECT_NAME`	Monitored host name

Attribute type		Item	Attribute name	Description
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Monitored host name
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Monitored host name	JP1_SOURCEHOST	Monitored host name

Legend:

--: None

(96) Event ID: Value specified for the ACTDEF parameter of the remote monitoring log file trap definition file

Attribute type		Item	Attribute name	Description
Basic attribute		Event ID	--	The value specified for the ACTDEF parameter
		Message	MESSAGE	Data content of one line in a log file
		Event issuing time	--	Time that the event was issued
Extended attribute	Common information	Event level	SEVERITY	Severity specified by the ACTDEF parameter in the action definition file
		Product name	PRODUCT_NAME	In Windows: • When the -p option is specified for the jcfallogdef command, the jcfallogstart command, and the startup option of remote monitoring: /HITACHI/JP1/NT_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option. • When the -p option is not specified for the jcfallogdef command, the jcfallogstart command, and the startup option for remote monitoring: /HITACHI/JP1/NT_LOGTRAP In UNIX: • When the -p option is specified for the jcfallogdef command, the jcfallogstart command, and the startup option for remote monitoring: /HITACHI/JP1/UX_LOGTRAP/*program-name*, where *program-name* is the log data output source program name specified by the -p option. • When the -p option is not specified for the jcfallogdef command, the jcfallogstart

Attribute type		Item	Attribute name	Description
				command, and the startup option for remote monitoring: /HITACHI/JP1/UX_LOGTRAP
		Object type	OBJECT_TYPE	LOGFILE
		Object name	OBJECT_NAME	Name of log file to be monitored
		Root object type	ROOT_OBJECT_TYPE	LOGFILE
		Root object name	ROOT_OBJECT_NAME	Name of log file to be monitored
	User-specific or program-specific information	Platform	PLATFORM	In Windows: NT In UNIX: UNIX
		PP name	PPNAME	/HITACHI/JP1/IM/REMOTE_MONITORING/LOGTRAP
		Host name	JP1_SOURCEHOST	Event source host name (Monitored host name)
		Monitoring ID	E.JP1_TRAP_ID#	ID number of a log file trap
		Monitoring name	E.JP1_TRAP_NAME#	Monitoring name

Legend:

--: None

#: An attribute that exists when the JP1/Base version of Manager is 10-50 or later.

(97) Details of event ID: 00003A71, or the event ID specified in the filter block of the remote-monitoring event log trap action-definition file

Attribute type		Item	Attribute name (WMI attribute name)	Description
Basic attribute		Event ID	B.ID	Event ID specified in the filter block of the remote-monitoring event log trap action-definition file. If no event ID is specified, the value is set to 00003A71.
		Message	B.MESSAGE (Message or InsertionStrings)	Event log message.[#1] A maximum of 1,023 bytes. If the limit is exceeded, the excess bytes are discarded.
		Event issuing time	--	Time that the event was issued
Extended attribute	Common information	Event level	E.SEVERITY (EventType)	Registration is according to the event log type: Error: Error Warning: Warning Information: Information, details, and other types of information Notice: Successful audit, failed audit
		Event source product name	E.PRODUCT_NAME (SourceName)	/HITACHI/JP1/NTEVENT_LOGTRAP/*source*
		Object type	E.OBJECT_TYPE	LOGFILE

Attribute type		Item	Attribute name (WMI attribute name)	Description
			E.ROOT_OBJECT_TYPE	
		Object name	E.OBJECT_NAME E.ROOT_OBJECT_NAME	NTEVENTLOG
	User-specific or program-specific information	Event log registration date and time	E.A0 (TimeGenerated)	time_t type (absolute time in seconds since UTC 1970-01-01 00:00:00)
		Computer name	E.A1 (ComputerName)	Computer name value *host-name.domain-name-displayed-when-hostname-command- executed*
		Type	E.A2 (Logfile)	Value indicating the event log type
		Type	E.A3 (Type)	Value corresponding to the event log level
		Category	E.A4 (CategoryString or Category)	Value for the event log task category
		Event ID	E.A5 (EventCode)	Value for the event log event ID
		User name	E.A6 (User)	Value for the event log user name
		Platform	E.PLATFORM	NT
		PP name	E.PPNAME	/HITACHI/JP1/IM/AGENTLESS/EVENTLOGTRAP
		Event source host name	E.JP1_SOURCEHOST#2	Monitored host name
		Log file trap name	E.JP1_TRAP_NAME	Log file trap name specified in the remote-monitoring event log trap action-definition file. Not output if unspecified (attribute does not exist).

Legend:

--: None

#1: If the message DLL in which the description of an event log is coded is not set correctly, the inserted phrase or the detail code is enclosed in double-quotation marks (") to register it in a JP1 event message.

#2: An attribute that exists only when the common definition (ATTR_EVENT_LOGTRAP_SOURCEHOST) is 1.

(98) Details of event ID: 00003F90

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	00003F90
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	Process ID of jco_spmd
	Registered time	TIME	Time of registration

Attribute type		Item	Attribute name	Description
		Arrived time	`ARRIVEDTIME`	Arrival time
		Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB3737-E The` *component-name managed-process-name* `terminated abnormally.`
Extended attribute	Common information	Event level	`SEVERITY`	`Error`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/SPMD`
		Object type	`OBJECT_TYPE`	`SPMD`
		Object name	`OBJECT_NAME`	Name of the process that terminated abnormally
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(99) Details of event ID: 00003F91

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	`00003F91`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of `jco_spmd`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535#

Attribute type		Item	Attribute name	Description
				• In UNIX 0
		Source group ID	`GROUPID`	• In Windows From -1 to 65,535# • In UNIX 0

		Source user name	`USERNAME`	• In Windows
				`SYSTEM`
				• In UNIX
				`root`

		Source group name	`GROUPNAME`	• In Windows Blank • In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	`MESSAGE`	`KAVB3613-W A` *component-name* `timeout occurred in` *managed-process-name*`. Processing continues.`
Extended attribute	Common information	Event level	`SEVERITY`	`Warning`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/SPMD`
		Object type	`OBJECT_TYPE`	`SPMD`
		Object name	`OBJECT_NAME`	Name of the process resulting in a start timeout
		Occurrence	`OCCURRENCE`	`NOTICE`

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, `-1` is set.

(100) Details of event ID: 00003F92

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	--	`00003F92`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	Process ID of `jco_spmd`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Arrival time
	Source user ID	`USERID`	• In Windows From -1 to 65,535# • In UNIX 0

Attribute type		Item	Attribute name	Description
		Source group ID	GROUPID	• In Windows From -1 to 65,535# • In UNIX 0
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows Blank • In UNIX root
		Event-issuing server name	SOURCESERVER	Name of the event-issuing server
		Source serial number	SOURCESEQNO	Source serial number
		Message	MESSAGE	KAVB3616-I Restart of the *component-name managed-process-name* has finished.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/SPMD
		Object type	OBJECT_TYPE	SPMD
		Object name	OBJECT_NAME	Name of the process that was restarted
		Occurrence	OCCURRENCE	NOTICE

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file of JP1/Base are set. If they are not specified, -1 is set.

(101) Details of event ID: 00006400

Attribute type	Item	Attribute name	Description
Basic attribute	Event ID	ID	00006400
	Serial number	SEQNO	Serial number#
	Reason for registration	REASON	Value from 1 to 4#
	Source process ID	PROCESSID	0
	Registered time	TIME	Registered time#
	Arrived time	ARRIVEDTIME	Arrival time#
	Source user ID	USERID	• In Windows# From -1 to 65535 • In UNIX# 0
	Source group ID	GROUPID	• In Windows#

Attribute type		Item	Attribute name	Description
				From -1 to 65535# - In UNIX# 0
		Source user name	USERNAME	- In Windows# SYSTEM - In UNIX# root
		Source group name	GROUPNAME	- In Windows# Blank - In UNIX# root
		Event-issuing server name	SOURCESERVER	Event-issuing server name#
		Target event server name	DESTSERVER	Target event server name#
		Source IP address	EVIPADDR	Event source IP address# - IPv4: The format is *aaa*.*bbb*.*ccc*.*ddd* (decimal values of 1-3 digits with no leading zeros). - IPv6: The format is *aaaa*:*bbbb*:*cccc*:*dddd*:*eeee*:*ffff*:*gggg*:*hhhh* (hexadecimal values of from 1 to 4 digits with no leading zeros).
		Destination IP address	--	Event destination IP address#
		Source serial number	SOURCESEQNO	Source serial number#
		Code set	--	Language code that JP1/IM - Manager is using#
		Message	MESSAGE	If the message was changed by the display message change function, the changed message is set. If the message was not changed, the message text of the original event is set.
		Detailed information	--	Not set
Extended attribute	Common information	Event level	SEVERITY	If the event level of the original event was changed by the severity changing function, the changed event level is set. If the event level was not changed, the original event's event level is set.
		User name	USER_NAME	Original event's USER_NAME
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/MO
		Object type	OBJECT_TYPE	Original event's OBJECT_TYPE
		Object name	OBJECT_NAME	Original event's OBJECT_NAME
		Root object type	ROOT_OBJECT_TYPE	Original event's ROOT_OBJECT_TYPE
		Root object name	ROOT_OBJECT_NAME	Original event's ROOT_OBJECT_NAME

Attribute type		Item	Attribute name	Description
		Object ID	`OBJECT_ID`	Original event's `OBJECT_ID`
		Occurrence	`OCCURRENCE`	Original event's `OCCURRENCE`
		Start time	`START_TIME`	Original event's `START_TIME`
		End time	`END_TIME`	Original event's `END_TIME`
		Return code	`RESULT_CODE`	Original event's `RESULT_CODE`
	Basic attribute of original event	Serial number	`B_SEQNO`	Original event's serial number
		Event ID	`B_ID`	Original event's event ID. The format is *basic-code*:*extended-code*. The basic code and extended code are hexadecimal values of up to 8 digits with no leading zeros.
		Reason for registration	`B_REASON`	Original event's reason for registration
		Source process ID	`B_PID`	Original event's source process ID
		Registered time	`B_DATE`	Sets the date portion of the original event's registered date and time in the format *YYYY*/*MM*/*DD*. The result is a character string that has been converted to the server's time zone.
			`B_TIME`	Sets the time portion of the original event's registered date and time in the format *hh*:*mm*:*ss*. The result is a character string that has been converted to the server's time zone.
		Arrived time	`B_ARVDATE`	Sets the date portion of the original event's arrival date and time in the format *YYYY*/*MM*/*DD*. The result is a character string that has been converted to the server's time zone.
			`B_ARVTIME`	Sets the time portion of the original event's arrival date and time in the format *hh*:*mm*:*ss*. The result is a character string that has been converted to the server's time zone.
		Source user ID	`B_USRID`	Original event's source user ID
		Source group ID	`B_GRPID`	Original event's source group ID
		Source user name	`B_USR`	Original event's source user name
		Source group name	`B_GRP`	Original event's source group name
		Event-issuing server name	`B_HOST`	Original event's event-issuing server name
		Destination event server name	`B_DESTSERVER`	Original event's destination event server name
		Source IP address	`B_IPADDR`	Original event's source IP address
		Destination IP address	`B_DESTIPADDR`	Original event's destination IP address
		Sequence number by source	`B_SRCNO`	Original event's sequence number by source

Attribute type		Item	Attribute name	Description
		Code set	B_CODESET	Original event's code set
		Message	B_MSG	Original event's message
		Detailed information	B_DETAIL	Original event's detailed information • If the detailed information is a character string: Set to the detailed information character string unchanged • If the detailed information is in binary format: Set to blank
	Extended attribute of original event: Common information	Event level	E_SEVERITY	Original event's SEVERITY (if the event level was changed by the severity changing function, the changed event level is set)
		Product name	E_PRODUCT_NAME	Original event's PRODUCT_NAME
	Extended attribute of original event: Program-specific information	Extended attribute of original event: Program-specific information	E_*	The original event's extended attribute program-specific information is set. These are items with E_ prefixed to the original event's attribute name. For example, if the original event's extended attribute name is PLATFORM and the content is NT, the event's attribute name after conversion will be E_PLATFORM, and the content will still be NT. However, if the original event's extended attribute name is 31 bytes long or greater, the E_ will be omitted from the converted event attribute name.
	JP1/IM - M program-specific information	Event source information	EVTSRC_INFO	• When the host mapping function is enabled in JP1/IM - Manager: Source host (E.JP1_SOURCEHOST) • When the host mapping function is disabled in JP1/IM - Manager: Event-issuing server name (B.SOURCESERVER)
		JP1/IM - MO version	MO_VERSION	1100
		Event source name	EVTSRC_NAME	• When E.JP1ADD_EVTSRC_NAME is in the original event: E.JP1ADD_EVTSRC_NAME • When E.JP1ADD_EVTSRC_NAME is not in the original event: Event-issuing server name (B.SOURCESERVER)
		Target system name	SYSTEM_NAME	• When E.JP1ADD_SYSTEM_NAME is in the original event: E.JP1ADD_SYSTEM_NAME

Attribute type		Item	Attribute name	Description
				• When E.JP1ADD_SYSTEM_NAME is not in the original event: In a non-Japanese language environment, ALLSYSTEM is set.
		Extended attribute storage result	ADDEXTATTR_RESULT	The extended attributes' storage result is set. The sum of the following values is set as a two-byte hexadecimal value. • 0: The values of all extended attributes were able to be stored. • 1: The maximum number of extended attributes (100) was reached, so some attributes could not be stored. • 2: The maximum total size of extended attributes (10 KB) was reached, so some attributes could not be stored. • 4: One or more extended attributes were stored without the E_ prefix because the maximum name length was exceeded. • 8: One or more extended attributes could not stored due to a naming conflict with other extended attributes.

Legend:

--: None

#: Set by JP1/Base.

Note: *Original event* refers to the event that JP1/IM - Manager acquired from JP1/Base.

(102) Details of event ID: 00003FE0

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FE0
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	From -1 to 65535[#1]
	Source group ID	GROUPID	From -1 to 65535[#1]
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows Blank

Attribute type		Item	Attribute name	Attribute value
				- In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Name of the event-issuing server
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	--	`KAJY22023-I The response action will now start. (suggestion ID :` *suggestion-ID*`, JP1 user name :` *JP1-user-name*`, IM management node :` *tree-SID*`, action information :` *action-information*`)`#2
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/DD`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`SUGGESTION`
		Occurrence	`OCCURRENCE`	`START`
	User-specific or program-specific information	Suggestion ID	`SUGGESTION_ID`	Suggestion ID of the response action
		Tree SID	`TREE_SID`	Tree SID of the response action#3

Legend:

--: None

#1: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

#2: If the message exceeds 1,024 bytes, only the characters up to 1,023 bytes are set. If the 1,023rd byte happens to constitute part of a multi-byte character, the message is set with that multi-byte character and the subsequent characters discarded.

#3: If the total size of the extended attributes exceeds 10,000 bytes, the value of this attribute is truncated to make the total size 10,000 bytes, with the last three bytes converted to an ellipsis (`...`).

(103) Details of event ID: 00003FE1

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	`00003FE1`
	Serial number	`SEQNO`	Serial number
	Source process ID	`PROCESSID`	`0`
	Registered time	`TIME`	Time of registration
	Arrived time	`ARRIVEDTIME`	Time of arrival
	Source user ID	`USERID`	From `-1` to `65535`#1
	Source group ID	`GROUPID`	From `-1` to `65535`#1

	Source user name	`USERNAME`	- In Windows
			`SYSTEM`
			- In UNIX
			`root`

	Source group name	`GROUPNAME`	- In Windows Blank

Attribute type		Item	Attribute name	Attribute value
				• In UNIX `root`
		Event-issuing server name	`SOURCESERVER`	Event-issuing server name
		Source serial number	`SOURCESEQNO`	Source serial number
		Message	--	`KAJY22024-I The response action has finished. (suggestion ID :` *suggestion-ID*`, JP1 user name :` *JP1-user-name*`, IM management node :` *tree-SID*`, action information :` *action-information*`)`#2
Extended attribute	Common information	Event level	`SEVERITY`	`Information`
		Product name	`PRODUCT_NAME`	`/HITACHI/JP1/IM/DD`
		Object type	`OBJECT_TYPE`	`SERVICE`
		Object name	`OBJECT_NAME`	`SUGGESTION`
		Occurrence	`OCCURRENCE`	`END`
	User-specific or program-specific information	Suggestion ID	`SUGGESTION_ID`	Suggestion ID of the response action
		Tree SID	`TREE_SID`	Tree SID of the response action#3

Legend:

--: None

#1: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

#2: If the message exceeds 1,024 bytes, only the characters up to 1,023 bytes are set. If the 1,023rd byte happens to constitute part of a multi-byte character, the message is set with that multi-byte character and the subsequent characters discarded.

#3: If the total size of the extended attributes exceeds 10,000 bytes, the value of this attribute is truncated to make the total size 10,000 bytes, with the last three bytes converted to an ellipsis (`...`).

(104) Details of event ID: 00003FF0

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF0
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	From -1 to 65,535#
	Source group ID	GROUPID	Fron -1 to 65,535#
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows NULL string

Attribute type		Item	Attribute name	Attribute value
				• In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63025-I The response action for an event was sent to the JP1/IM - Manager that manages response-action execution hosts. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		Start time	START_TIME	Time sent to JP1/IM - Manager managing Response Action execution destination
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "SENDED"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execution Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(105) Details of event ID: 00003FF1

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF1
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	From -1 to 65,535#

Attribute type		Item	Attribute name	Attribute value
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	- In Windows SYSTEM - In UNIX root
		Source group name	GROUPNAME	- In Windows NULL string - In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63026-I The JP1/IM agent management base was requested to execute the response action for an event. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		Start time	START_TIME	Time sent to JP1/IM agent management base
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "RUNNING"
		Action Description	EXECCMD	- For restapi URL of RESTAPI - For cmd Commands the execution requested
		Execution Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(106) Details of event ID: 00003FF2

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF2

Attribute type		Item	Attribute name	Attribute value
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63027-I Execution of the response action for an event ended. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database, return code = termination-code)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "ENDED"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execution Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(107) Details of event ID: 00003FF3

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003FF3
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows NULL String • In UNIX root
		Event-issuing server name	SOURCESERVE R	Event-issuing server name
		Source serial number	SOURCESEQN O	Source serial number
		Message	--	KAJY63028-E The response action for an event ended abnormally. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NA ME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STAT US	Action's Status "ERROR" (for Fail) or "FAIL" (for failed communication or execution failed)
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execution Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(108) Details of event ID: 00003FF4

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003FF4
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63029-I The response action for a response-action status notification event was sent to the JP1/IM - Manager that manages response-action execution hosts. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		Start time	START_TIME	Time sent to JP1/IM - Manager managing Response Action execution destination
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "SENDED"
		Action Description	EXECCMD	• For restapi

Attribute type		Item	Attribute name	Attribute value
				URL of RESTAPI • For cmd Commands the execution requested
		Execution Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(109) Details of event ID: 00003FF5

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003FF5
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	From -1 to 65,535#
		Source group ID	GROUPID	From -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group name	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63030-I The JP1/IM agent management base was requested to execute the response action for a response-action status notification event. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action

Attribute type		Item	Attribute name	Attribute value
		Start time	START_TIME	Time sent to JP1/IM agent management base
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "RUNNING"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(110) Details of event ID: 00003FF6

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF6
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	From -1 to 65,535#
	Source group ID	GROUPID	From -1 to 65,535#
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group name	GROUPNAME	• In Windows NULL string • In UNIX root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	KAJY63031-I Execution of the response action for a response-action status notification event ended. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database, return code = termination-code)

Attribute type		Item	Attribute name	Attribute value
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "ENDED"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(111) Details of event ID: 00003FF7

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF7
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#
	Source group ID	GROUPID	For -1 to 65,535#
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
	Event-issuing server name	SOURCESERVER	Event-issuing server name

Attribute type		Item	Attribute name	Attribute value
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63032-E The response action for a response-action status notification event ended abnormally. (sequence number in integrated monitoring database = sequence-number-in-integrated-monitoring-database)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "ERROR" (for Fail) or "FAIL" (for failed communication or execution failed)
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(112) Details of event ID: 00003FF8

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF8
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#
	Source group ID	GROUPID	For -1 to 65,535#
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root

Attribute type		Item	Attribute name	Attribute value
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63033-W Although execution of a response action was requested, a response-action status notification event cannot be issued because the information about the response action does not exist in the ResponseAction results-management database. (detailed information = detailed-information)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		Start time	START_TIME	Time sent to JP1/IM agent management base
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "RUNNING"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(113) Details of event ID: 00003FF9

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003FF9
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival

Attribute type		Item	Attribute name	Attribute value
		Source user ID	USERID	For -1 to 65,535#
		Source group ID	GROUPID	For -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63034-W Although execution of a response action ended, a response-action status notification event cannot be issued because the information about the response action does not exist in the ResponseAction results-management database. (detailed information = detailed-information)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "ENDED"
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(114) Details of event ID: 00003FFA

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003FFA
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	For -1 to 65,535#
		Source group ID	GROUPID	For -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63035-E Although a response action ended abnormally, a response-action status notification event cannot be issued because the information about the response action does not exist in the ResponseAction results-management database. (detailed information = detailed-information)
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Object ID	OBJECT_ID	Serial number of the event that caused the action
		End time	END_TIME	Time when Response Action finished
		Occurrence	OCCURRENCE	NOTICE
	User-specific or program-specific information	Action executing host	EXECHOST	Host name Response Action execution perform to
		Action Status	ACTION_STATUS	Action's Status "ERROR" (for Fail) or "FAIL" (for failed communication or failed Execute)
		Action Description	EXECCMD	• For restapi URL of RESTAPI • For cmd Commands the execution requested

Attribute type		Item	Attribute name	Attribute value
		Execute Destination SID	EXECSID	The SID of the configuration of the system which Response Action executes (JP1/IM agent control base or JP1/IM - Manager)

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, -1 is set.

(115) Details of event ID: 00003FFB

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003FFB
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	For -1 to 65,535#
		Source group ID	GROUPID	For -1 to 65,535#
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY63023-I The response action automatic execution function was activated by loading autoResponseAction definitions. The loaded definitions will take effect for the processing of the next-received event and the following events. (number of definitions = number-of-valid-definitions / total-number-of-definitions-in-a-definition, last-received event' arrival time = arrival-time-of-the-last-processed-event (YYYY/MM/DD HH:MM:SS), sequence number in integrated monitoring database = integrated-monitoring-DB-serial-number-of-the-last-processed-event)
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	RESPONSEACTION
		Occurrence	OCCURRENCE	RUN

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(116) Details of event ID: 00003F80

Attribute type		Item	Attribute name	Attribute value
Basic attribute		Event ID	--	00003F80
		Serial number	SEQNO	Serial number
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	For -1 to 65,535[#]
		Source group ID	GROUPID	For -1 to 65,535[#]
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY02073-I Generation of the information related to IM management nodes ended normally.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	NODE
		Occurrence	OCCURRENCE	END

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(117) Details of event ID: 00003F81

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003F81
	Serial number	SEQNO	Serial number

Attribute type		Item	Attribute name	Attribute value
		Source process ID	PROCESSID	0
		Registered time	TIME	Time of registration
		Arrived time	ARRIVEDTIME	Time of arrival
		Source user ID	USERID	For -1 to 65,535[#1]
		Source group ID	GROUPID	For -1 to 65,535[#1]
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY02074-E Failed to generate the information related to IM management nodes. (return value = return-value, details = details)[#2]
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	NODE
		Occurrence	OCCURRENCE	Error

Legend:

--: None

#1: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

#2: If the message is 1,024 bytes or more, a string truncated to 1,023 bytes or less is set. If byte 1,023 is in the middle of a multibyte character, that character is also truncated.

(118) Details of event ID: 00003F82

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003F82
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535[#]

Attribute type		Item	Attribute name	Attribute value
		Source group ID	GROUPID	For -1 to 65,535[#]
		Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
		Source group ID	GROUPNAME	• In Windows NULL string • In UNIX root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY02075-I Processing to apply the information related to IM management nodes ended normally.
Extended attribute	Common information	Event level	SEVERITY	Information
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	NODE
		Occurrence	OCCURRENCE	END

Legend:

--: None

#: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(119) Details of event ID: 00003F83

Attribute type	Item	Attribute name	Attribute value
Basic attribute	Event ID	--	00003F83
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrived time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535[#1]
	Source group ID	GROUPID	For -1 to 65,535[#1]
	Source user name	USERNAME	• In Windows SYSTEM • In UNIX root
	Source group ID	GROUPNAME	• In Windows NULL string • In UNIX

Attribute type		Item	Attribute name	Attribute value
				root
		Event-issuing server name	SOURCESERVER	Event-issuing server name
		Source serial number	SOURCESEQNO	Source serial number
		Message	--	KAJY02076-E Failed to apply the information related to IM management nodes. (return value = return-value, details = details)#2
Extended attribute	Common information	Event level	SEVERITY	Error
		Product name	PRODUCT_NAME	/HITACHI/JP1/IM/DD
		Object type	OBJECT_TYPE	SERVICE
		Object name	OBJECT_NAME	NODE
		Occurrence	OCCURRENCE	END

Legend:

--: None

#1: The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

#2: If the message is 1,024 bytes or more, a string truncated to 1,023 bytes or less is set. If byte 1,023 is in the middle of a multibyte character, that character is also truncated.

3.2.3 Lists of JP1 events output by JP1/IM - Agent

(1) Attributes of JP1 events that monitor and issue performance data

The following is a list of attributes of JP1 events that monitor and issue performance data.

Table 3–3: List of attributes of JP1 events that monitor and issue performance data

Category	Item	Name Attribute	Description
Basic attributes	Event ID	ID	Value# with Setup to entry "jp1_pc_eventid" in alert configuration file (jpc_alerting_rules.yml) #: If the jp1_pc_eventid is not Setup, 00007600 is Setup.
	Message	MESSAGE	• When a firing condition of the alert is met A string generated from the value set in item "jp1_pc_firing_description" in the alert configuration file (jpc_alerting_rules.yml).# #: If you have not set a jp1_pc_firing_description, "The alert is firing. (`alert=`*alert name*)" is set. • When the alert firing condition is no longer met A string generated from the value set in item "jp1_pc_resolved_description" in the alert configuration file (jpc_alerting_rules.yml)# #: If you have not set a jp1_pc_resolved_description, "The alert is resolved. (`alert=`*alert name*)" is set.
Extended Properties (Common	Severity	SEVERITY	• When a firing condition of the alert is met

Category	Item	Name Attribute	Description
Information)			Value set in item "jp1_pc_severity" of alert configuration file (`jpc_alerting_rules.yml`)# #: If you have not set a jp1_pc_severity, set an empty character. • When the alert firing condition is no longer met `Information`
	Product Name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2` or `/HITACHI/JP1/JPCCS2/`*xxxx* *xxxx* is your preferred Value.
	Object Type	OBJECT_TYPE	`ALARM`
	Object Name	OBJECT_NAME	Alert name# #: Value with Setup to entry "alert" in alert configuration file (jpc_alerting_rules.yml)
	Event Type	OCCURRENCE	`NOTICE`
	Origin host name	JP1_SOURCEHOST	Setup Value depends on whether or not it is the alert of judging Yet another cloudwatch exporter performance-data. • For Yet another cloudwatch exporter For metric performance data in EC2, you Setup Value that is Setup in the jp1_pc_nodelabel tag of AWS as Event source host. If you have not set a jp1_pc_nodelabel, set the empty character. For a metric other than EC2, Host name of integrated agent that is Setup in Yet another cloudwatch exporter discovery configuration file field targets is Setup as Event source host. If targets are not set, set the empty character. • Other than Yet another cloudwatch exporter Setup the monitored Host name of field targets in the Discovery configuration file as event source host. If targets are not set, set the empty character. If file entry "targets" in Blackbox exporter (ICMP monitoring) discovery configuration is set to IP address as Setup, set IP address to Setup as Event source host.
Extended Attribute (Unique Information)	PP Name	PPNAME	`/HITACHI/JP1/JPCCS2`
	Alert firing time	JPC_TIME	Stores the duration of alert firing in seconds since UTC 1970-01-01 00:00:00. In the event extension attribute definition file included with JP1/IM - Manager, specify "type="elapsed_time/date_format:CLIENT" on the attr statement. For a resolved alert, it is the same as the time of the firing alert. For details, see the description of "*type = "elapsed_time/date_format:CLIENT*" in *Definition file for extended event attributes* (*company-name_product-name*`_attr_`*xx*`.conf`) in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.
	Host name for integrated agent	JPC_PROMETHEUS	Value set in item "jp1_pc_prome_hostname" of Prometheus configuration file (`jpc_prometheus_server.yml`)# # If you have not set a jp1_pc_prome_hostname, set an empty character.
	Scrape Jobs	JPC_JOB	In the scrape_configs of the Prometheus configuration file (`jpc_prometheus_server.yml`), the value set for job_name
	jp1_pc_nodelabel	JPC_NODELABEL	In the scrape_configs of the Prometheus configuration file (`jpc_prometheus_server.yml`), the value set for item "jp1_pc_nodelabel"# # If you have not set a jp1_pc_nodelabel, set the empty character.
	Exporter Name	JPC_EXPORTER	Value set in item "jp1_pc_exporter" in the discovery configuration file#

Category	Item	Name Attribute	Description
			Note # If not specified, it will be "Unknown Exporter".
	Metric Name	JPC_METRICNAME	The value set in item "jp1_pc_metricname" of the alert configuration file (`jpc_alerting_rules.yml`)# # If you have not set a jp1_pc_metricname, set an empty character.
	jp1_pc_remote_monitor_instance	JPC_REMOTE_ MONITOR_INSTANCE	Value set in item "jp1_pc_remote_monitor_instance" in the discovery configuration file# Note # If not specified, the attribute is not set.
	AWS Service Name	JPC_AWS_SERVICE	AWS service name Set only for Yet another cloudwatch exporter performance data. Set the service name corresponding to the metric name set in item "jp1_pc_metricname" in the alert setting file (`jpc_alerting_rules.yml`) by searching for it from the metric definition file. If you have not set a jp1_pc_metricname, set an empty character.
	AWS account	JPC_AWS_ACCOUNT	AWS account string Set only for Yet another cloudwatch exporter performance data. This string corresponds to the AWS account ID described in the AWS definition file (`aws_settings.conf`). If the definition does not exist, set "default".
	AWS Region name	JPC_AWS_REGION	AWS region name monitored by Yet another cloudwatch exporter Set only for Yet another cloudwatch exporter performance data. Note # If dimension_InstanceId label does not exist, set it to an empty character.
	AWS InstanceId	JPC_AWS_DIM_INSTANCEID	AWS/EC2 dimension names Set the label only if dimension_InstanceId exists in the performance data of Yet another cloudwatch exporter.
	AWS FunctionName	JPC_AWS_DIM_FUNCTIONNAME	AWS/Lambda dimension names Set the label only if dimension_FunctionName exists in the performance data of Yet another cloudwatch exporter.
	AWS Resource	JPC_AWS_DIM_RESOURCE	AWS/Lambda dimension names Set it only if dimension_Resource label exists in the performance data of Yet another cloudwatch exporter.
	AWS BucketName	JPC_AWS_DIM_BUCKETNAME	AWS/S3 dimension names Yet another cloudwatch exporter's performance data dimension_BucketName so set the label only if it exists.
	AWS StorageType	JPC_AWS_DIM_STORAGETYPE	AWS/S3 dimension names Set the label only if dimension_StorageType exists in the performance data of Yet another cloudwatch exporter.
	AWS FilterId	JPC_AWS_DIM_FILTERID	AWS/S3 dimension names Set dimension_FilterId label only if it exists in the performance data of Yet another cloudwatch exporter.
	AWS TableName	JPC_AWS_DIM_TABLENAME	AWS/DynamoDB dimension names Set the label only if dimension_TableName exists in the performance data of Yet another cloudwatch exporter.
	AWS StateMachineArn	JPC_AWS_DIM_STATEMACHINEARN	AWS/States dimension names Set it only if dimension_StateMachineArn label exists in the performance data of Yet another cloudwatch exporter.

Category	Item	Name Attribute	Description
	AWS QueueName	JPC_AWS_DIM_QUEUENAME	AWS/SQS dimension names Set the dimension_QueueName label only if it exists in the performance data of Yet another cloudwatch exporter.

	Component name	JPC_COMPONENT	Component Name
			Setup JP1 event which product plugin in JP1/IM - Agent is related.
			• For jp1pccs_azure.js
			`/HITACHI/JP1/JPCCS/AZURE/CONFINFO`
			• For jp1pccs_kubernetes.js
			`/HITACHI/JP1/JPCCS/KUBERNETES/CONFINFO`
			• For jp1pccs.js
			"/HITACHI/JP1/JPCCS/CONFINFO" or Null

(2) JP1 event issued that monitoring a textual log File

This JP1 event is issued when fluentd monitors the text-format log File and a log that Match the user-specified condition is output. For fluentd, see *3.15.3 Log monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 3–4: Attributes for JP1 Events Issued by Monitoring Text-Format Log File

Classification	Item	Attribute name	Description
Basic attributes	Event ID	ID	Value specified for JP1 Event ID in monitoring text-formatted log file definition file. The default Value is "00007601".
	Message	MESSAGE	Value captured by the name MESSAGE in text-formatted log file monitoring definition file's regular expressions for parsing logging.
Extended Properties (Common Information)	Event level	SEVERITY	Value specified in Event level of monitoring text-formatted log file definition file.
	Product name	PRODUCT_NAME	Label-name of `/HITACHI/JP1/JPCCS2/LOGTRAP/ IM management node`
	Object type	OBJECT_TYPE	`LOGFILE`
	Object name	OBJECT_NAME	File of the logged File.
	Root object type	ROOT_OBJECT_TYPE	`LOGFILE`
	Root object name	ROOT_OBJECT_NAME	File of the logged File.
Extended Attribute (Unique Information)	Platform	PLATFORM	In Windows :NT In Linux: UNIX
	PP	PPNAME	`/HITACHI/JP1/JPCCS2`
	Event source host	JP1_SOURCEHOST	Host name of the logged host. In Logical host, Logical host name.
	Log file trap name	JP1_TRAP_NAME	Value specified in Log file trap name of monitoring text-formatted log file definition file.

Classification	Item	Attribute name	Description
	The Date/time logs added	JPC_LOG_TIME	Value captured by the name "time" in monitoring text-formatted log file definition file's regular expressions for parsing logging. If not, Date/time that Fluentd monitored for logging. Time_t type (seconds since UTC 1970-01-01 00:00:00)
	jp1_pc_nodelabel	JPC_NODELABEL	Value specified in label name of IM management node for monitoring text-formatted log file definition file.
	Any item	Any attribute name	Any Value. You can capture Message of the log and Setup any Value for any Attribute name. For details on setting method, see the description of the `[Attributes Settings]` section in the *Monitoring text-formatted log file definition file (fluentd_@@trapname@@_tail.conf.template)* in *Chapter 2. Definition Files* in the *JP1/Integrated Management 3 - Manager Command, Definition File and API Reference*.

(3) JP1 event to be issued by monitoring Windows event log

This is a JP1 event that is issued when fluentd monitors Windows event log and a log that Match the user-specified criteria is output. For fluentd, see *3.15.3 Log monitoring function by JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 3–5: List of JP1 Event Attributes to Issue Monitoring Windows Event Logs

Classification	Item	Attribute name	Description
Basic attributes	Event ID	ID	Value specified for JP1 Event ID in monitoring Windows event-log definition file. The default Value is "00007602".
	Message	MESSAGE	Message of Windows event log. Limit: 1023 bytes. The excess is displayed as a truncation.
Extended Properties (Common Information)	Event level	SEVERITY	Add according to what is displayed in the "Levels" or "Keywords" section of Windows's Event Viewer. The following shows what Event level displays: • `Critical: Critical` • `Error: Error` • `Warning: Warning` • `Information: Information, details, etc.` • `Notice: Success Audit, Failure Audit`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2/LOGTRAP/ Sources` Sources indicate what is displayed in Windows's Event Viewer under "Sources", i.e. Provider text of the render property (or ProviderName's Value if it cannot be converted).
	Object type	OBJECT_TYPE	`LOGFILE`
	Object name	OBJECT_NAME	`NTEVENTLOG`
	Root object type	ROOT_OBJECT_ TYPE	`LOGFILE`
	Root object name	ROOT_OBJECT_NAME	`NTEVENTLOG`

Classification	Item	Attribute name	Description
Extended Attribute (Unique Information)	The Date/time logs added	A0	Date/time displayed in the "Log Date" section of Windows's Event Viewer. time_t type (seconds since UTC 1970-01-01 00:00:00)
	Computer name	A1	This is what is displayed in "Computer" in the event viewer of Windows.
	NT Logging type"	A2	`System/Security/Application/Setup/Directory Service/DNS Server/File Replication Service/Internet Explorer/Key Management Service/HardwareEvents` In addition, the information displayed in "Log Name" in the Event Viewer of Windows.
	NT Logging Type	A3	`Critical/Error/Warning/Information/Verbose/Audit_Success/Audit_Failure` (determined by Value of level, keyword)#
	NT Logging Categories	A4	This is what is displayed in the "Task Category" of the Event Viewer of Windows. (Task rendered text) Unable to convert to rendered string: (Value of Task) If it cannot be classified: None
	NT Event ID	A5	This is what is displayed in "Event ID" in the event viewer of Windows.
	NT User name	A6	This is what is displayed for "Users" in the event viewer of Windows.
	NT logging level	A7	This is what is displayed in "Levels" in the event viewer of Windows.
	NT Logging Keywords	A8	This is what is displayed in "Keywords" in the event viewer of Windows.
	NT logging opcode	A9	This is what is displayed in "Opcode" in the event viewer of Windows.
	Platform	PLATFORM	`NT`
	PP	PPNAME	`/HITACHI/JP1/JPCCS2`
	Event source host	JP1_SOURCEHOST	Host name of the logged host. For Logical host, Logical host name.
	Log file trap name	JP1_TRAP_NAME	Value specified for the Log file trap name for monitoring Windows event-log definition file.
	jp1_pc_nodelabel	JPC_NODELABEL	Value specified in the label name of IM management node for monitoring Windows event-log definition file.

#

NT logging type Setup is shown below.

- When NT Logging type" is Security
  Based on keyword's Value, Setup the following NT logging types in the format "Value of keyword : Setup String".
  0x10000000000000:Audit_Success, 0x20000000000000:Audit_Failure
  If the bitwise AND of Value is not 0, Setup string is Attribute value. If both are 0, "-" is Setup as Value.
- When NT Logging type" Is Not Security
- Based on level's Value, we Setup the following NT logging types in the format "Value of level : Setup String".
  1: Critical, 2:Error, 3:Warning, 4:Information, 5:Verbose, et al. : Information

(4) JP1 Events Issued When JP1/IM agent control base is Disconnected

This JP1 event is issued when there is no connection from JP1/IM agent control base to JP1/IM agent management base for a certain period of time using polling monitoring function of JP1/IM agent control base. For details about JP1/IM agent control base's polling monitoring function, see *3.15.8 Polling monitoring of JP1/IM agent management base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 3–6: List of attributes for JP1 events issued when JP1/IM agent control base is disconnected

Classification	Item	Attribute name	Description
Basic attributes	Event ID	ID	00007620
	Message	MESSAGE	KNBC20043-E
Extended Properties (Common Information)	Event level	SEVERITY	`Error`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`
	Object type	OBJECT_TYPE	`IMAGTHC`
	Object name	OBJECT_NAME	`IMAGENT`
	Occurrence	OCCURRENCE	`NOTICE`
Extended Attribute (Unique Information)	Event source host	JP1_SOURCEHOST	Integrated agent host name on which JP1/IM agent control base has been installed that JP1/IM agent management base has not been connected for a period of time.

(5) JP1 Events to Issue When JP1/IM agent control base Is Connected

This JP1 event is issued when JP1/IM agent control base connects to JP1/IM agent management base using polling monitoring function of JP1/IM agent control base. For details about JP1/IM agent control base's polling monitoring function, see *3.15.8 Polling monitoring of JP1/IM agent management base* in *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 3–7: List of attributes for JP1 events that are issued when JP1/IM agent control base is connected

Classification	Item	Attribute name	Description
Basic attributes	Event ID	ID	00007621
	Message	MESSAGE	KNBC20044-I
Extended Properties (Common Information)	Event level	SEVERITY	`Information`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`
	Object type	OBJECT_TYPE	`IMAGTHC`
	Object name	OBJECT_NAME	`IMAGENT`

Classification	Item	Attribute name	Description
	Occurrence	OCCURRENCE	NOTICE
Extended Attribute (Unique Information)	Event source host	JP1_SOURCEHOST	Integrated agent host name where JP1/IM agent control base connected to JP1/IM agent management base is installed.

(6) JP1 Events Issue When JP1/IM agent control base Stops on Normal

This JP1 event is issued when JP1/IM agent control base is stopped by polling monitoring function of JP1/IM agent control base. For details about JP1/IM agent control base's polling monitoring function, see *3.15.8 Polling monitoring of JP1/IM agent management base* in *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Table 3–8: List of attributes for JP1 events that are issued when JP1/IM agent control base is stopped normally

Classification	Item	Attribute name	Description
Basic attributes	Event ID	ID	00007622
	Message	MESSAGE	KNBC20045-I
Extended Properties (Common Information)	Event level	SEVERITY	Information
	Product name	PRODUCT_NAME	/HITACHI/JP1/JPCCS2
	Object type	OBJECT_TYPE	IMAGTHC
	Object name	OBJECT_NAME	IMAGENT
	Occurrence	OCCURRENCE	NOTICE
Extended Attribute (Unique Information)	Event source host	JP1_SOURCEHOST	Integrated agent host name on which JP1/IM agent control base to be stopped is installed.

(7) JP1 Events Issue When Add of agent is detected

Table 3–9: List of attributes for JP1 events that are issued when add for agent is detected

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is "00007630" [#1].
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0

Classification	Item	Attribute name	Description
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535[#2]
	Source group ID	GROUPID	For -1 to 65,535[#2]
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	KNBC00030-I
Extended attribute (Common Info)	Event level	SEVERITY	Information
	Product name	PRODUCT_NAME	/HITACHI/JP1/JPCCS2
	Object type	OBJECT_TYPE	SERVICE
	Object name	OBJECT_NAME	IMBASE
	Occurrence	OCCURRENCE	NOTICE

Legend: --: None

#1

This JP1 event is tied to the manager node. In a configuration with more than one manager, only the directly connected manager node is associated with it.

#2

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(8) JP1 Events Issue When Deletion of agent is detected

Table 3–10: List of attributes for JP1 events that are issued when deletion for agent is detected

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is the "00007631" [#1].
	Serial number	SEQNO	Serial number

Classification	Item	Attribute name	Description
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535[#2]
	Source group ID	GROUPID	For -1 to 65,535[#2]
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	KNBC00031-I
Extended attribute (Common Information)	Event level	SEVERITY	Information
	Product name	PRODUCT_NAME	/HITACHI/JP1/JPCCS2
	Object type	OBJECT_TYPE	SERVICE
	Object name	OBJECT_NAME	IMBASE
	Occurrence	OCCURRENCE	NOTICE

Legend: --: None

#1

This JP1 event is tied to the manager node. In a configuration with more than one manager, only the directly connected manager node is associated with it.

#2

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(9) JP1 Events Issues when Updating agent Info is Detected

Table 3–11: List of attributes for JP1 events issue when updating agent data is detected

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is the "00007632" [#1].

Classification	Item	Attribute name	Description
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#2
	Source group ID	GROUPID	For -1 to 65,535#2
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	KNBC00032-I
Extended attribute (Common Information)	Event level	SEVERITY	Information
	Product name	PRODUCT_NAME	/HITACHI/JP1/JPCCS2
	Object type	OBJECT_TYPE	SERVICE
	Object name	OBJECT_NAME	IMBASE
	Occurrence	OCCURRENCE	NOTICE

Legend: --: None

#1

This JP1 event is tied to the manager node. In a configuration with more than one manager, only the directly connected manager node is associated with it.

#2

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(10) JP1 Events to be Issued on a Successful Deletion of Defined Files

Table 3–12: List of attributes for JP1 events that are issued when Deletion of File is successful

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is "00007640".
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration

Classification	Item	Attribute name	Description
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535[#]
	Source group ID	GROUPID	For -1 to 65,535[#]
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	Setup one of the following: • KNBC20015-W • KNBC20016-W • KNBC20017-W • KNBC20018-W • KNBC00018-I
Extended attribute (Common Information)	Event level	SEVERITY	`Infomation`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`
	Object type	OBJECT_TYPE	`SERVICE`

	Object name	OBJECT_NAME	When the definition file of JP1/IM - Manager was operated:
			`FILEOPERATION_MANAGER`
			When the definition file of integrated agent was operated:
			`FILEOPERATION_AGENT`

	Occurrence	OCCURRENCE	`NOTICE`

Legend: --: None

#

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(11) JP1 Events to Issue When Deletion of definition Files Fail

Table 3–13: List of attributes for JP1 events that are issued when Deletion of definition Files fail

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is "00007641".
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#
	Source group ID	GROUPID	For -1 to 65,535#
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	Setup one of the following: • KNBC00012-E • KNBC00013-E • KNBC00015-E • KNBC00017-E • KNBC00010-E • KNBC00014-E • KNBC20009-E • KNBC20012-E • KNBC20014-E • KNBC20023-E
Extended attribute (Common Information)	Event level	SEVERITY	`Error`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`
	Object type	OBJECT_TYPE	`SERVICE`

	Object name	OBJECT_NAME	When the definition file of JP1/IM - Manager was operated:
			`FILEOPERATION_MANAGER`
			When the definition file of integrated agent was operated:
			`FILEOPERATION_AGENT`

Classification	Item	Attribute name	Description
	Occurrence	OCCURRENCE	`NOTICE`

Legend: --: None

#

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(12) JP1 Events to Issue When definition File is Updated Successfully

Table 3–14: List of attributes for JP1 events issue when File is successfully updated

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is "00007642".
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#
	Source group ID	GROUPID	For -1 to 65,535#
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	Setup one of the following: • KNBC20020-W • KNBC20021-W • KNBC20016-W • KNBC20017-W • KNBC20019-E • KNBC00019-I
Extended attribute (Common Information)	Event level	SEVERITY	`Infomation`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`

Classification	Item	Attribute name	Description
	Object type	OBJECT_TYPE	`SERVICE`

	Object name	OBJECT_NAME	When the definition file of JP1/IM - Manager was operated:
			`FILEOPERATION_MANAGER`
			When the definition file of integrated agent was operated:
			`FILEOPERATION_AGENT`

	Occurrence	OCCURRENCE	`NOTICE`

Legend: --: None

#

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

(13) JP1 Events to Issue When Updating definition files Fail

Table 3–15: List of attributes for JP1 events that are issued when updating definition Files fail

Classification	Item	Attribute name	Description
Basic attributes	Event ID	--	The default Value is "00007643".
	Serial number	SEQNO	Serial number
	Source process ID	PROCESSID	0
	Registered time	TIME	Time of registration
	Arrival time	ARRIVEDTIME	Time of arrival
	Source user ID	USERID	For -1 to 65,535#
	Source group ID	GROUPID	For -1 to 65,535#
	Source user name	USERNAME	In Windows: SYSTEM In UNIX: root
	Source group name	GROUPNAME	In Windows: NULL string In UNIX: root
	Event-issuing server name	SOURCESERVER	Event-issuing server name
	Source serial number	SOURCESEQNO	Source serial number
	Message	--	Setup one of the following: • KNBC20009-E • KNBC20012-E

Classification	Item	Attribute name	Description
			• KNBC20014-E • KNBC20022-E • KNBC20023-E • KNBC00012-E • KNBC00013-E • KNBC00015-E • KNBC00016-E • KNBC00010-E • KNBC00014-E
Extended attribute (Common Information)	Event level	SEVERITY	`Error`
	Product name	PRODUCT_NAME	`/HITACHI/JP1/JPCCS2`
	Object type	OBJECT_TYPE	`SERVICE`

	Object name	OBJECT_NAME	When the definition file of JP1/IM - Manager was operated:
			`FILEOPERATION_MANAGER`
			When the definition file of integrated agent was operated:
			`FILEOPERATION_AGENT`

	Occurrence	OCCURRENCE	`NOTICE`

Legend: --: None

#

The substitute user ID and substitute group ID specified in the event server settings file are set. If they are not specified, `-1` is set.

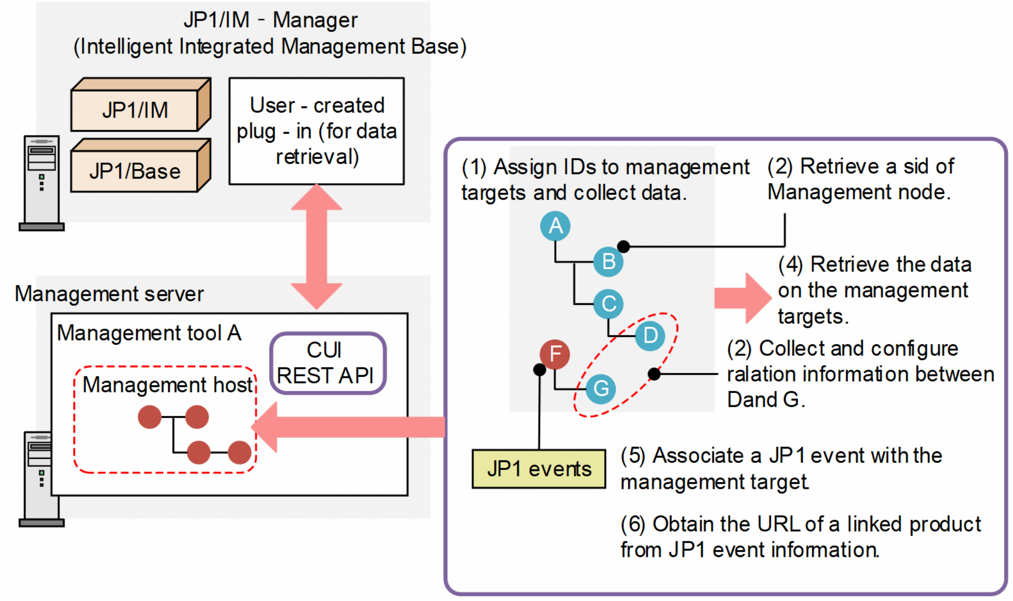
4 User-created Plug-ins

In JP1/IM - Manager (Intelligent Integrated Management Base), the users can perform some operations with their own plug-ins. This chapter describes the user-created plug-ins.

4.1 What a user can do with the user-created plug-in

The user can create a plug-in and retrieve information from the management tool of a linked product, to manage it with the Intelligent Integrated Management Base. The following figure shows the operations provided by the user-created plug-in.

Figure 4–1: Operations provided by the user-created plug-in



JP1/IM - Manager
(Intelligent Integrated Management Base)
JP1/IM
JP1/Base
User - created plug - in (for data retrieval)
Management server
Management tool A
CUI
REST API
Management host
(1) Assign IDs to management targets and collect data.
(2) Retrieve a sid of Management node.
A
B
C
D
F
G
(4) Retrieve the data on the management targets.
(2) Collect and configure ralation information between Dand G.
JP1 events
(5) Associate a JP1 event with the management target
(6) Obtain the URL of a linked product from JP1 event information.

The following describes the flow using numbered steps (the numbers correspond to the numbers in the figure).

1. Assign IDs to targets managed by management tool A and collect data.
2. Collect and configure relation information between D and G.
3. Retrieve the tree SID of the IM management node.
4. Retrieve the data on management targets.
5. Associate a JP1 event with the management target to manage the status of the target#.
6. Obtain the URL of a linked product from JP1 event information to open the window of the linked product.

#: As an assumption, the management target must issue a JP1 event to manage its status.

4.1.1 Format of the user-created plug-in

The user-created plug-in is written in JavaScript and provides its functionality in the CommonJS module format. The following example shows the format of a user-created plug-in and how to write a method called when configuration information is retrieved.

Format

```
module.exports = {
          operations-of-the-user-created-plug-in
};
```

Example

```
module.exports = {
          // Operations performed when configuration information is retrie
ved
          __configurationGet : function(args) {
                 // Determine if the configuration collection should be pr
ocessed with args.component
                 if (args.component !== "/HITACHI/JP1/PP/CONFINFO") {
                         return;
                 }
                 // If yes:
                 // When args.data contains configuration information in J
SON format, pass it as it is
args.setResult(args.data);
          },
};
```

The following shows the rules for writing the user-created plug-in:

- Plug-in file name: *product-name*`.js`
  Example: `jp1pfm.js, jp1ajs.js`
- Encoding: ASCII
- Language: English
  Comments must also be in English.
- Supported line feed code
  CR, LF, CR+LF

> **Important**
>
> When a user creates a new method, the name of the method must not start with an underscore.

4.2 Setting up and considering the management target

Before adding a new target managed by JP1/IM - Manager (Intelligent Integrated Management Base), you need to set up and consider the management target.

4.2.1 Adding a host

If you add a management target as a managed host, you need to add an additional host setting to the following definition files:

- System node definition file (`imdd_systemnode.conf`)
- Target host definition file for configuration collection (`imdd_target_host.conf`)

For details about the definition files, see *System node definition file (imdd_systemnode.conf)* and *Target host definition file for configuration collection (imdd_target_host.conf)* in *Chapter 2. Definition Files*.

4.2.2 Considering the SID

When adding the management target, you need to assign an SID that represents the target. For details on the SID, see *7.1 SID*.

In this section, the following hosts are used as examples of the management targets for description:

- Host A where management tool A is running
- Agent host B managed by management tool A

Specify SIDs as follows:

- Class of the SID for indicating any SID related to management tool A: `_ToolA-M_`
- Class of the SID for indicating a host: Use the reserved word `_HOST_`
- SID of the host where management tool A is running: `_ToolA-M_hostA/_HOST_hostA`
- Class of the SID for any agent host managed by host A: `_ToolA-A_`
- SID that represents host B: `_ToolA-M_hostA/_ToolA-A_hostB/_HOST_hostB`

Important

Define the class of an SID with a given string starting with an underscore (_) and ending with an underscore (_). In addition, `_JP1`, a string starting with `_HITACHI`, and another string starting with `_ROOT_`, `_SYSTEM_`, `_CATEGORY_`, `_SUBCATEGORY_`, or `_OBJECT_` are not available. The class is case insensitive.

If you use a JP1 event to manage the status of a monitoring target, you need to create the SID of the management node from the data of the JP1 event. Check to see if you can create the SID from the data of the JP1 event before considering the SID.

4.2.3 Considering data labeled "value" of the SID

You can add additional information labeled value to the assigned SID. JP1/IM - Manager (Intelligent Integrated Management Base) provides the variables listed in the following table.

Table 4–1: Variable names and their values

No.	Variable name	Value
1	component	Specifies the name of the product that manages the management target and the name of the product's component. SYSTEM, DEFAULT, and a string starting with HITACHI are reserved words and therefore cannot be specified. You can use ASCII numbers, uppercase alphabetic letters, and a forward slash (/). The value must be within 240 bytes. Example /VENDOR/TOOLA
2	category#	Specifies the category information that corresponds to each component (categoryId).
3	subCategory	Specifies the subcategory, such as a product name. This value can be up to 255 characters (any characters except control characters).
4	label	Specifies the name after a change, if the component name displayed in the tree is to be changed.
5	methods	Specifies the names of plug-in functions, in array format, that are executable through the plug-in processing execution REST API for the applicable component.

#

Specify the categoryId defined in the category name definition file for IM management nodes (imdd_category_name.conf) by using up to 255 half-width alphanumeric characters.

If you specify a category other than a standard category, add a definition to the category name definition file for IM management nodes. For details on the definition file, see *Category name definition file for IM management nodes (imdd_category_name.conf)* in *Chapter 2. Definition Files*.

The following table lists category IDs that the category variable can accept.

Table 4–2: Category IDs that the category variable can accept

No.	Category display name	Category ID to be specified
1	Job	job
2	Service Response	serviceResponse
3	Enterprise	enterprise
4	Transaction Processing	transactionProcessing
5	Application Server	applicationServer
6	Database	database
7	Platform	platform
8	Service	service
9	Virtual Machine	virtualMachine
10	Management Applications	managementApplications
11	Other Applications	otherApplications
12	Arbitrary category display name	Arbitrary category

The following shows an example in which `up` is added as `categoryId` and `User Program` as `categoryName`.

```
{
"meta":{
    "version":"1"
    },
    "categoryData":[
       {"categoryId":"job","categoryName":"Job"},
       {"categoryId":"serviceResponse","categoryName":"Service Response"},
       {"categoryId":"enterprise","categoryName":"Enterprise"},
       {"categoryId":"transactionProcessing","categoryName":"Transaction Pro
cessin"},
       {"categoryId":"applicationServer","categoryName":"Application Server"
},
       {"categoryId":"database","categoryName":"Database"},
       {"categoryId":"platform","categoryName":"OS"},
       {"categoryId":"service","categoryName":"Service"},

       {"categoryId":"virtualMachine","categoryName":"Virtual Machine"},
       {"categoryId":"otherApplications","categoryName":"Other Applications"
},
       {"categoryId":"up","categoryName":"User Program"}
    ]
}
```

4.3 Retrieving information from the management target

You can retrieve information from a management target in one of the following ways:

- Adapter command
- REST API

The adapter command is executed only once.

The creation of an adapter command is mandatory.

4.3.1 Collecting information with the adapter command

If you create a user-created plug-in and retrieve information from a management target in JP1/IM - Manager (Intelligent Integrated Management Base), you need an adapter command together with the plug-in. You execute the adapter command only once. You execute the adapter command several times and cannot acquire information. In addition, the adapter command has a one-to-one relationship with the user-created plug-in.

The adapter command communicates with the Intelligent Integrated Management Base via the standard input and output. When started from the Intelligent Integrated Management Base, the adapter command sends a response to the Intelligent Integrated Management Base via the standard output.

(1) Return values

The adapter command gives back the summary of an operation result as a return value.

Table 4–3: Return values of the adapter command

No.	Return value	Description
1	`0`	Successful completion
2	`1` to `49`	These values are assigned to an error when a warning occurs. (For example, a failure to collect part of information)
3	`50` to `99`	These values are assigned to a temporary error of the operation that can be retried.
4	`100` to `149`	Invalid environment (such as an incorrect version)
5	`150` to `199`	Program error

You can also add a return value specific to the adapter command within the range of the return values. The details of an error at runtime of the adapter command must be returned separately via the standard error output.

(2) Execution directory

The directory where the adapter commands is located as the execution directory.

(3) Input/output

Arguments, the standard input, the standard output, and the standard error output are used for data communication between the adapter command and the Intelligent Integrated Management Base.

The standard input and standard output of the adapter command is made up of *common header* and *data body*. The *data body* contains the information passed from the adapter command to the Intelligent Integrated Management Base.

The format is as follows:

```
Common header<Line feed code (<CR><LF> or <LF>)>Data body
```

The structure of the header is shown below. The header is expressed in CSV format.

```
protocol-name,protocol-version,character-code,program-product-name
```

The following table lists the details of the header:

No.	Name	Data type	Value to be specified
1	*protocol-name*	string	`JBSPGCMD`
2	*protocol-version*		Specify the same version as the *version of the adapter command settings file*#. Example `12000000`
3	*character-code*		Specify one of the following character codes based on the execution environment of the adapter command: • `8859_1` • `SJIS` • `MS932` • `EUCJIS` • `UTF-8` • `GB18030`
4	*program-product-name*		Specify the same value as the *component identifier*#.

#
For details, see *7.3.2 Adapter command settings file*.

If an error occurs during execution of the adapter command, the details are printed to the standard error output. Configure the details to be printed in ASCII characters.

(4) Notes

- The following commands are not available as the adapter command:
  - Command that requires a sub-entry command (interactive operation)
  - Command that involves escape sequences and control codes
  - Command that opens a window at the location where the command is executed
  - Command that does not end, such as a daemon
- The user may start more than one instance of the adapter command at the same time. If starting two or more instances of the adapter command simultaneously is not allowed, add an exclusive operation of its own to the command so that it returns a busy response when the second instance is started.
- Data cannot be sent and received simultaneously via the standard input and output. The adapter command that receives a request via the standard input must start sending response data after receiving all the request data.
- The adapter command is executed under the following permissions:

- In Windows: `SYSTEM`
- In UNIX: `root`

- A timeout period is set on the adapter command. Thus, the response must be returned before the command times out. The timeout period is 60 minutes.

(5) Adapter command settings file

An adapter command settings file is used to specify the name of the file for the adapter command. The naming rule is as follows:

```
name-of-the-component-specified-for-Adapter_SID.conf
```

Example

When the *name-of-the-component-specified-for-Adapter_SID* is `/VENDOR/TOOLA`:

```
Adapter_VENDOR_TOOLA.conf
```

The adapter command settings file is located at:

In Windows:

JP1/Base-installation-folder`\plugin\conf`

In UNIX:

`/opt/jp1base/plugin/conf`

The table below lists the setting items of the adapter command settings file. Use a tab or white space character to separate a label and its value.

Table 4–4: Setting items of the adapter command settings file

No.	Item	Label	Value to be specified
1	Version of the adapter command settings file	`fileversion`	`12000000`
2	Path to the adapter command	`cmdpath`	Specify the absolute path to the adapter command, including the command name. You do not have to enclose the path with double quotation marks or other characters.
3	Product that links with the adapter command	`upperpp`	`/HITACHI/JP1/IM/DD`
4	Type of the adapter command	`componenttype`	`JDD_CONFINFO`

The following shows a setting example of the adapter command settings file:

```
fileversion      12000000
cmdpath         C:\Program Files (x86)\Hitachi\jp1pc\bin\jp1getconfinfo.exe
upperpp         /HITACHI/JP1/IM/DD
componenttype   JDD_CONFINFO
```

Important

- A single line can contain a maximum of 4,096 characters.

- If there is more than one label with the same name, an error occurs.
- If the required label is not specified, an error occurs.
- If even a single error exists in the file, the file is no longer valid.
- The file is terminated with the line feed character.
- The file can contain ASCII characters only.
- When you specify a label, a white space or tab character is not allowed at the beginning of the row.
- Any row containing white space or tab characters only is ignored.

4.3.2 Retrieving information with the REST API

If you use the `jp1Imdd.callRest` method in the `__configurationGet` method of a user-created plug-in, you can execute any REST API. For details on the `jp1Imdd.callRest` method, see *jp1Imdd.callRest* in *4.5.1 Methods available in the user-created plug-in*.

4.4 Methods implemented in the plug-in

You implement the user-created plug-in that processes only what it can deal with by referring to the parameter values. If something is beyond the operation of the plug-in, it should return at once. In this case, avoid calling a method, such as the setError method.

4.4.1 Format of methods you can implement

The following table lists and describes the format of methods that you can implement in the user-created plug-in.

Table 4–5: Format of the method to be provided

No.	Item	Name	Description
1	Method name	--	The name of each method
2	Parameters	args	See the description of each method.
3	Return values	None	
4	Exception	None	Use the args.setError method, instead of an exception, to notify an error. For details, see *4.4.4(1) __configurationGet method*.

4.4.2 Implementation conventions of user-created plug-ins

The following shows the implementation conventions of user-created plug-ins:

- If JP1/IM receives a request from a user or a system that uses REST APIs, it always calls the method that corresponds to the request without being aware of the plug-ins.
- The plug-in refers to parameter information of methods and processes only those that can be processed by it. If the plug-in cannot process the methods, use return immediately without calling the setError method or logging the error.

  This is because if you call the setError method without using return immediately, the next plug-in will not be called and the call operation will exit.
- Whether a plug-in can be processed is basically determined by the sid value of the parameter. If you need to determine it based on information other than sid, see each method.

4.4.3 Language conventions of user-created plug-ins

If you pass lang (language information) to a method of a user-created plug-in, the language setting of the WWW browser is passed to it when you execute the method from the window of JP1/IM, and the value specified in the Accept-Language header of the HTTP request is passed to it when you execute the method from a REST API.

Make the user-created plug-ins work in Japanese mode when ja or ja-JP is specified or in English mode if en is specified.

Define how each user-created plug-in works if a value other than these values is specified. If lang is omitted or any undefined value is specified, make the plug-ins work as if en is specified.

4.4.4 List of methods

The table below lists and describes the methods to be implemented in the user-created plug-in.

You do not have to implement all the methods. Choose the methods you need for each product and implement them. For details about the plug-in methods provided by different products, see the respective manuals supplied with the products.

Table 4–6: List of methods implemented in the user-created plug-in

No.	Category	Method name	Description	Number in *4.1*[#2]
1	Get configuration information	`__configurationGet`	The method to collect the configuration information	1
2		`__configurationGetAdapterless`	Method to retrieve configuration information (when the adapter command has not been set up)	
3		`__createTreeNode`	The method to collect tree information	
4	Event	`__eventGet`	The method to process JP1 events	5
5		`__transformEvent`	This method converts event data (generated by an external system) to JP1 events.	
6	Get relation information	`__createLink`	The method to generate a relation between collected configurations.	2
7		`__linkValueGet`	The method to collect the details of link information	
8		`__simtLoad`	A method that collects related information needed when IM management node is loaded.	
9	Get trend information	`__metricListGet`	The method to get the list of metrics for time-series data that can be collected	3
10		`__timeSeriesDataGet`	The method to collect time-series data	
11	Get url information	`__urlGet`	The method to get the URL for starting a monitor	6
12	Any method created by the user#1	Any method created by the user[#1]	An arbitrary method created by the user. Avoid the method name starting with an underscore (_).	3

#1

The arbitrary method created by the user is executed via the plug-in processing execution API (`im_api_v1_actions`). For details on the plug-in processing execution API (`im_api_v1_actions`), see *5.7.1 Plug-in processing execution*.

#2

The numbers in this column correspond to the numbers in *4.1 What a user can do with the user-created plug-in*.

(1) __configurationGet method

Description

The method returns the configuration information of each product in JSON format. When host name is written to target host definition file for configuration collection (imdd_target_host.conf), in the Intelligent Integrated Management Base, call this method only when checking the return value of the adapter command after it is called and finding the value is `0`.

- If the configuration information is collected successfully

  In the `__configurationGet` method, call the `args.setResult` (configuration information in JSON format) method.

- If the method fails to collect the configuration information

  Call the `args.setError` (error message) method, instead of the `args.setResult` method.

In the `__configurationGet` method, either the `args.setResult` or `args.setError` method must be called if the `__configurationGet` method can process the component.

The `__configurationGet` method is called within the `jddcreatetree` command that creates the system management tree of the Intelligent Integrated Management Base.

Each user-created plug-in should refer to the value of `args.component` to determine if the plug-in can deal with the component.

Parameters

The following table lists and describes the parameters of the `__configurationGet` method.

Table 4–7: Parameters of the __configurationGet method

No.	Member	Description	Remarks
1	`hostname`	Name of the host from which the configuration information is collected	None
2	`component`	Name of the component managing the configuration information	`"/HITACHI/JP1/PFM/CONFINFO"`
3	`data`	Execution result of the adapter command. It is a string converted into UTF-8 format, based on the character code in the header information. The header information is not included.	None
4	`jp1UserName`	JP1 user name	The user has the administrator permissions for each product.
5	`jp1Token`	JP1 token for `jp1UserName`	The JP1 token is BASE64 encoded.
6	`protocolName`	Protocol name	The header information contained in the execution result of the adapter command
7	`protocolVersion`	Protocol version	The header information contained in the execution result of the adapter command
8	`codeset`	Character code	The header information contained in the execution result of the adapter command
9	`productName`	Product name	The header information contained in the execution result of the adapter command
10	`setResult(String json)`	The method to set the configuration information in JSON format	None
11	`setError(String message)`	The method for error notification. It sets an error message.	
12	`stderr`	It stores the value output by the adapter command to the standard error output.	

Note

You need to assign an SID with the `value` information added for each component to the configuration information that is set for `setResult`. For details on the SID, see *7.1 SID*.

List of configuration information to be returned

The following describes the list of configuration information returned by the `__configurationGet` method.

Formats

```
{
  "meta":{
    "timestamp":"created-time(ISO8601-formatted-UTC-time)",
    "objectRoot":[
        {
           "type":"object-root-node-type",
           "defaultSystem":
           {
             "name":"name-of-the-structured-identifier-of-the-default-s
ystem-node",
             "label":"display-name-of-the-default-system-node"
           }
        },...
                   ]
          },
    "simtData":[
             {"sid":"<SID>","value":{structured identifier}},
    ...
                 ]
}
```

Describe

The following table lists and describes what is contained in the list of obtained infrastructures.

Table 4–8: Description in the list of obtained infrastructures

No.	Item	Data types	Description
1	`meta`	Object	An object that stores file information
2	`timestamp`	string	Returns the date and time of file creation as the UTC time in ISO8601 format. This attribute cannot be omitted. The time is the server time of JP1/IM - Manager.
3	`objectRoot`	array	An array that stores the object root node type and the default system node information. This attribute can be omitted.
4	`type`	string	Indicates the object root node type (such as a network device (`NETWORKDEVICE`) or storage (`STORAGE`)) placed under the root node of the tree and under the system node. The host (`HOST`) does not have to be specified. Make sure that it is placed under the root node of the tree and under the system node. This attribute can be omitted. If it is omitted, only the host is placed under the root node of the tree and under the system node.
5	`defaultSystem`	Object	Specify the attribute if you create a default system node whose parent node is the object root node. If this attribute is omitted, the default tree node of the object root node specified in `type` is placed directly under `AllSystems`.
6	`name`	string	Specifies the name of the configuration information SID for the default system node. If this attribute is omitted, the object root node type is set as the SID name of configuration information.
7	`label`	string	Specifies the label of the default system node. If this attribute is omitted, the `label` attribute is not set for the additional information of the default system node.
8	`simtData`	array	An array of configuration information
9	`sid`	string	Indicates the configuration information SID.

No.	Item	Data types	Description
10	value	Object	Indicates a structured identifier

Example

For details on the information the __configurationGet method retrieves from each product, see *7.1.4 Information retrieved from each product*.

Impact of configuration information set by setResult

The following table lists and describes the functions that are affected by the configuration information set by setResult and its impact.

Table 4–9: List of affected functions

No.	Function	Impact
1	System status monitoring	• The IM management node acquisition function outputs the set configuration information as an IM management node file. • The IM management node tree generation function# uses the configuration information to generate a tree and outputs it as an IM management node tree file. • The __eventGet method uses the SID of the configuration information. With the __eventGet method, a JP1 event is mapped with an IM management node.
2	Integrated monitoring of systems by IM management nodes	__createLink or the IM management node link definition file (imdd_nodeLink_def.conf) uses the SID of the configuration information. Workflows are displayed according to IM management node links with type of rootJobnetExecutionOrder (root jobnet execution order).
3	Custom UI display	A custom UI window is displayed according to the SID of the configuration information.
4	Related node display	__createLink or the IM management node link definition file (imdd_nodeLink_def.conf) uses the SID of the configuration information. Related nodes are displayed according to IM management node links.
5	IM management node property display	The information specified in property of the additional information (value) of the configuration information is displayed.
6	Startup of a linked product window	The window of a linked product is opened for the IM management node in which __urlGet is specified in methods of the additional information (value) of the configuration information.
7	Trend information display	Trend information on the specified metric is displayed for the IM management node in which __metricListGet and __timeSeriesDataGet are specified in methods of the additional information (value) of the configuration information.
8	Managing Trend Data by IM management node	Refer to the jp1im_TrendData_labels of the configuration information grant information (value), and specify the value of replacement string "$jp1im_TrendData_labels" specified in PromQL expression in the argument promQLQuery of jp1TrendDataService.getTrendData method. If the jp1im_TrendData_labels of the configuration information is not specified, trend data related to the applicable managed node cannot be acquired. For details of jp1TrendDataService.getTrendData method, see *4.5.17 jp1TrendDataService.getTrendData*.

#

For details on the IM management node tree generation function, see *7.4 IM management node tree generation function*.

(2) __configurationGetAdapterless method

Description

Similar to the __configurationGetAdapterless method, this method returns the configuration of the application in JSON format. Implement and use this method if you cannot implement adapter commands, such as monitoring SaaS. Intelligent Integrated Management Base invokes this method if you do not write host name in target host definition file for configuration collection (imdd_target_host.conf) only.

If you want to implement this method on each user-created plug-in, refer to value of args.component to determine if it can be processed.

The specific environment information required to implement this method (for example, information related to authentication when monitoring SaaS) is described in file defined in user-created plug-in. For details, see *4.6.1 Definition files used by user-created plug-ins*.

Parameters

The following table lists and describes the parameters of the `__configurationGetAdapterless` method.

Table 4–10: Parameters of the __configurationGetAdapterless method

No.	Member	Description	Remarks
1	`component`	Component name from which the configuration information is managed	"/HITACHI/JP1/PFM/" + Product name specified in product of the configuration target definition file (imm_target_host.comf)
2	`jp1UserName`	JP1 user name	User with administrator privileges for each product
3	`jp1Token`	jp1UserName JP1 token	JP1 tokens are BASE64 encoded
4	`setResult(String json)`	Method that sets JSON form of the configuration	None
5	`setError(String message)`	Methods for Error Notifications Sets an error message.	

Note

For the configuration information to be specified to setResult, SID must be added with value information for each component. For details of SID, see *7.1 SID*.

- When acquisition of configuration information ends normally

  Invoke the args.setResult in __configurationGetAdapterless method (JSON format configuration information).

- When acquisition of configuration information fails

  Call args.setError (error message) method instead of args.setResult method.

In the __configurationGetAdapterless method, if the component can be processed by itself, be sure to call either args.setResult method or args.setError method.

The __configurationGetAdapterless method is called in jddcreatetree command that creates Intelligent Integrated Management Base system-managed tree.

List of configuration information to be returned

The format of retrieving the list of configuration information returned by the __configurationGetAdapterless method, the description, and the effect of the configuration information set by setResult are the same as those of the __configurationGet method.

When to use the __configurationGet method properly

The main differences between the __configurationGet and __configurationGetAdapterless methods are listed below.

Table 4–11: __configurationGet and __configurationGetAdapterless methods compared

Method name	Configuration acquisition target definition Description in file	Method for obtaining unique environment information	Remarks
__configurationGet	Products and host name	Adapter command or user-created plug-in definition file	JP1/Base is required
__configurationGetAdapterless	Product only	User-created plug-in definition file	None

Therefore, the __configurationGet method and the __configurationGetAdapterless method are used differently as shown in the tables below.

Table 4–12: Use of the __configurationGet and __configurationGetAdapterless methods

Usage method name	Use case
__configurationGet	• If you do not want to include environmental data in product plugin definition file (for security or other reasons)
__configurationGetAdapterless	• If you cannot install JP1/Base • When it is difficult to implement adapter commands (when you do not need to use adapter commands)

(3) __createTreeNode method

Description

The method collects the tree SID that corresponds to `simtData` in the input information together with additional information, and returns them in JSON format.

If a user-created plug-in implements the `__createTreeNode` method, the default tree of JP1/IM can be customized. For details on the default tree, see *7.4.2 Node generation function*.

The user-created plug-in generates a tree node object and sets it with `setResult` if the tree SID of `simtData` is the target of the tree node to be customized. If `simtData` objects have identical values in both the object type and name of the target, they will be the same node in the tree. Therefore, configure `simtData` objects that have identical values in both the object type and name to return the same tree SID.

If you do not customize the parent node of the tree node to be customized, use the `treeNodeCreator` object to get the tree SID of the parent node portion and use it as a part of the tree SID.

- If the tree SID and additional information can be retrieved successfully

  Call the `args.setResult` (tree SID in JSON format) method within the `__createTreeNode` method.

- If the tree SID and additional information cannot be retrieved

  Call the `args.setError` (error message) method, not the `args.setResult` method.

If the `__createTreeNode` method itself can process SimtData, make sure to call either the `args.setResult` method or `artgs.setError` method within the `__createTreeNode` method.

The `__createTreeNode` method is called in the `jddcreatetree` command that creates a system management tree for the Intelligent Integrated Management Base.

Parameters

The following table lists and describes the parameters of the `__createTreeNode` method.

Table 4–13: Parameters of the __createTreeNode method

No.	Member	Description	Remarks
1	`jp1UserName`	The JP1 user name	None
2	`jp1Token`	A JP1 authentication token that corresponds to `jp1UserName`	
3	`simtData`	`SimtData` of which you want to get the tree SID	
4	`treeNodeCreator`	An object that provides the functions to manage information of created nodes and create a default tree. For details, see *4.4.4(3)(a) treeNodeCreator object*.	
5	`setResult (String json)`	The method to set the retrieved tree SID and additional information in JSON format	
6	`setError (String message)`	The method for error notification. It sets an error message.	

Format of the tree SID and additional information to be returned

The following describes the format of the tree SID and additional information returned by the `__createTreeNode` method.

Formats

```
{
    "meta":{
        "componentName":"name-of-the-component-from-which-tree-informat
ion-is-retrieved"
    },
    "simtData":[
        {"sid":"tree-SID","value":{structured-identifier}},
        ...
   ]
}
```

Describe

The following table lists and describes the items of the retrieved tree SID and additional information.

Table 4–14: Items of the retrieved tree SID and additional information

No.	Item	Data types	Description
1	`meta`	Object	Indicates meta information.
2	`componentName`	string	Indicates the name of the component from which the tree information is retrieved.
3	`simtData`	Object	Indicates a simtData
4	`sid`	string	Indicates a tree SID
5	`value`	Object	Indicates a structured identifier

Example

The following shows an example of retrieving information with the `__createTreeNode` method.

```
{
    "meta":{
        "componentName":"/HITACbHI/JP1/OA/CONFINFO"
    },
    "simtData":[
        {
           "sid":"_ROOT_AllSystems/_HOST_host1/_CATEGORY_job
           /_SUBCATEGORY_JP1%2FAJS3%20-%20Manager/_OBJECT_AJSROOT1",
           "value":
             {
                "target":["_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_AJSROOT1"
],
                "label":"AJSROOT1"}}
             }
        }
    ]
}
```

Impact of IM management node tree information set by setResult

The following table lists and describes the function that is affected by the IM management node tree information set by `setResult` and its impact.

Table 4–15: List of affected functions

No.	Function	Impact
1	System status monitoring	IM management node information is merged with tree information generated by the IM management node tree generation function# and output as an IM management node tree file.

#

For details on the IM management node tree generation function, see *7.4 IM management node tree generation function*.

(a) treeNodeCreator object

The `treeNodeCreator` object provides the `getObjectRootTreeSID`, `getHostNameDef`, and `getCategoryName` methods.

(b) getObjectRootTreeSID method

The `getObjectRootTreeSID` method returns the tree SID that corresponds to `target` (SID) specified in the parameter. Use this method when you do not customize the parent node of an object node, and then use the return value as a part of the tree SID of the object node.

Parameters

The following table lists and describes the parameters of the getObjectRootTreeSID method.

Table 4–16: Parameters of the getObjectRootTreeSID method

No.	Item	Data types	Description
1	target	string	Configuration information SID for the object root node corresponding to the parent node of the tree node to be customized
2	objectRoot	Object[]	Object root node information Use the format below. `[{"type":"`*object-root-node-type*`"},,,},`#...`]`

#

You can specify information in the object in the same format as `meta.objectRoot` of configuration information that is retrieved by the `__configurationGet` method. For details, see *4.4.4(1) __configurationGet method*.

Return values

The method returns the tree SID that corresponds to `target`. The return values vary depending on how the tree node is generated when the `getObjectRootTreeSID` method is called.

Table 4–17: Return values of the getObjectRootTreeSID method

No.	How the tree node is generated	Return values
1	If the tree node has already been generated	The method returns the generated tree SID that corresponds to `target`.
2	If the tree node has not been generated	The method analyzes the content of `target` and generates the tree SID that is based on the definitions in the system node definition file (`imdd_systemnode.conf`) and the host name definition file (`imdd_host_name.conf`). If the content does not match the definition in the system node definition file (`imdd_systemnode.conf`), the method returns the default tree SID.

For details about the system node definition file, see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files*.

(c) getHostNameDef method

The `getHostNameDef` method returns the host name definition that corresponds to `hostName` specified in the parameter, according to the host name definition file (`imdd_host_name.conf`). Use this method if you customize the tree for the `HOST` node, and then use the return values as a name and label of the tree SID of the `HOST` node.

Parameters

The following table lists and describes the parameters of the getHostNameDef method.

Table 4–18: Parameters of the getHostNameDef method

No.	Item	Data types	Description
1	hostName	string	Specifies the host name (alias name).

Return values

The `getHostNameDef` method returns the following value according to the definition in the host name definition file (`imdd_host_name.conf`):

```
{"hostName":"value-in-the-definition-file","label":"value-in-the-definitio
n-file"}
```

The method returns null if there is no corresponding host name definition.

For details about the host name definition file, see *Host name definition file (imdd_host_name.conf)* in *Chapter 2. Definition Files*.

(d) getCategoryName method

The `getCategoryName` method returns the category name that corresponds to `category` (ID) specified in the parameter. Use this method if the tree to be customized contains a `CATEGORY` node, and then use the return value as a label of the tree SID.

Parameters

The following table lists and describes the parameters of the getCategoryName method.

Table 4–19: Parameters of the getCategoryName method

No.	Item	Data types	Description
1	category	string	ID of `category`

Return values

The `getCategoryName` method returns the category name that corresponds to `category`, according to the category name definition file for IM management nodes (`imdd_category_name.conf`).

The method returns null if there is no corresponding category name definition.

For details about the category name definition file for IM management nodes, see Category name definition file for *IM management nodes (imdd_category_name.conf)* in *Chapter 2. Definition Files*.

(4) __eventGet method

Description

This method returns the configuration information SIDs corresponding to all JP1 events issued by each product. Each user-created plug-in must return the configuration information SID to the individual JP1 events issued by the corresponding product. Each user-created plug-in refers to the value, such as `args.productName`, and determines that the plug-in itself can deal with the event.

- If a configuration information SID has been successfully generated for each one of the issued JP1 events:
  Call the `args.setTargetSid` (configuration information SID) method in the `__eventGet` method.
- If an attempt to generate a configuration information SID corresponding to an issued JP1 event fails due to missing data in the JP1 event:
  Without calling the `args.setError` (error message) method, return from the method and exit the process.

The `__eventGet` method is called when the Intelligent Integrated Management Base gets the JP1 event.

Parameters

The following table lists and describes the parameters of the `__eventGet` method.

Table 4–20: Parameters of the __eventGet method

No.	Member	Description	Remarks
1	`productName`	Product name	None
2	`idBase`	Event ID	Decimal number
3	`event`	JP1 event information	`event.sid`: SID of the JP1 event `event.value`: Data labeled `value` of the JP1 event#
4	`setTargetSid(String sid)`	Method that sets a configuration information SID corresponding to each JP1 event	None
5	`setError(String message)`	The method for error notification. It sets an error notification.	

#

The data labeled `value` contains various attribute names and attribute values of the event. You can use the following format to retrieve the attribute value for an attribute name:

`value['`*property-name*`']`

Put `B.` for a basic attribute or `E.` for an extended attribute in front of the attribute name.

Example: `value['E.JPC_MGR']`

Impact of SID information with setTargetSid set for it

The following table lists and describes the function that is affected by the SID information with setTargetSid set for it and its impact.

Table 4–21: List of affected functions

No.	Function	Impact
1	System status monitoring	The JP1 event is mapped to the IM management node whose configuration information SID is target. If you execute the jddupdatetree command in configuration change mode, the host name information provided in the configuration information SID returned with this method is used to determine the host to which to remap the JP1 event that has a configuration information SID that has been deleted from the configuration.

(5) __transformEvent method

Description

This method converts JSON format data to JP1 events.

The __transformEvent method, which is implemented in user-created plug-in, or product plugin, can convert an external system-generated event received in JP1 event transformation API into a JP1 event.

Parameters

The following table lists and describes the parameters of the __ transformEvent method.

Table 4–22: Parameters of the __transformEvent

No.	Member	Description
1	eventData	Event information received from the linked product (JSON format)
2	jp1eventmax	Maximum number of JP1 events that can be issued
3	setResult(String json)	Method for setting JP1 events (JSON format) converted from event information received from linked products
4	setError(String message)	Methods for error notification Set the error code and message.

When using __transformEvent method in a plug-in, it is necessary to implement it so that the __transformEvent method determines whether the data of the input event information is data to be processed by the plug-in.

In addition, depending on the judgment result, it is necessary to implement the JP1 event to be returned to be set to setResult only when the data should be processed by the plug-in. If the data is not to be processed by your plug-in, return it without setting anything.

The JP1 event to be set to setResult returned by the __transformEvent method is set in the following format.

The format of the returned JP1 event is checked by the caller's JP1 event conversion API. If malformed, the JP1 event conversion API outputs a KAJY67000-W message in the response body.

In addition, JP1 events exceeding 100 cannot be issued. If more than 100 JP1 events are set in setResult, JP1/IM - Manager issues up to 100 events from the beginning of the JP1 event sequence and does not issue subsequent events. In the plug-in, please be able to determine the details of events that were not issued by outputting them to a log.

Note that __transformEvent method does not check whether the value of the attribute for the JP1 event to be created is invalid or not. If the value of the attribute is invalid, JP1/IM - Manager's JP1 event conversion API will fail, and the JP1 event with the error will not be issued.

Format of JP1 event to be returned

Format

```
{
  "pluginName":Plug-in name,
  "exceedJp1eventMaxDetected":Detection of exceeding the upper limit of th
e number of converted JP1 events
  "events":[
    {
      "eventId":Event ID,
      "message":Message,
      "attrs":{Extended attribute name: Extended attribute value, ...}
    },
    ...
  ]
}
```

Parameters

No	Item name	Data type	Description
1	`pluginName`	`String`	Sets a string that represents the plug-in. Used to generate error messages in JP1 event conversion API#. This field cannot be omitted.
2	`exceedJp1eventMaxDetected`	`boolean`	Set whether or not to detect that the number of converted JP1 events exceeds the upper limit. • If the limit is exceeded: `true` • Otherwise: `false` This field cannot be omitted. If this item is `true`, the JP1 event conversion API# sets `KAJY67003-W` in the response body.
3	`events`	`Array`	Set the JP1 event to be issued in an array. The maximum number of events you can set is 100. The plug-in using this method determines whether the upper limit has been exceeded, and if the upper limit is exceeded, set the item `exceedJp1eventMaxDetected` to `true` and return it to the caller.
4	`eventId`	`Array`	Set the basic event ID to be issued within the following range. • 0 - 1FFFF • 7FFF8000 - 7FFFFFFF This field cannot be omitted. If a value outside the range is specified, JP1 Event Conversion API# sets `KAJY67000-W` in the response body and `The eventId specification is out of range. Set the specified value to a value in the range of 0 - 1FFF, 7FFF8000 - 7FFFFFFF.` as the factor.
5	`message`	`Array`	Set the message text that represents the contents of the JP1 event. This field cannot be omitted. The character encoding of the message to be registered depends on the character encoding of the OS environment where JP1/IM - Manager is located. Set as a string of up to 1,023 bytes. If a character string of 1,024 bytes or more is specified, a character string of up to 1,023 bytes is set to the message of the JP1 event.
6	`attrs`	`String`	Specify an array of extended attribute names. This field is optional.

No	Item name	Data type	Description
			If the same extended attribute name is specified more than once, it is overwritten by the value of the last extended attribute specified. Extended attribute names can be names that begin with uppercase letters and contain up to 32 bytes of uppercase letters, numbers, and underscore (_) lines. If the character string to be constructed is invalid, set `KAJY67000-W` in the response body of JP1 Event Conversion API* and set `The extended attribute name of attrs is invalid. Please specify uppercase letters and first letters.` as the factor. When a character string exceeding 32 bytes is specified, the JP1 event conversion API[#] sets `KAJY67000-W` as the response body and sets `The extended attribute name of attrs must be a string of 32 bytes or less.` as the factor. Also, do not specify the prefix `E.` for extended attribute names. When `E.` is specified, the JP1 event conversion API[#] sets `KAJY67000-W` as the response body and `The extended attribute name of attrs is invalid. Please specify uppercase letters and first letters.` as the factor. The total length of all extended attribute values can be up to 10,000 bytes. If the total length limit is exceeded, the JP1 event conversion API[#] sets `KAJY67000-W` as the response body and `The upper limit of the extended attribute value of attrs is 10000 bytes. Specify a string of 10000 bytes or less.` as the factor. For details on JP1 event attributes, see *3.1 Attributes of JP1 events*.

Note #

For details of JP1 event conversion API, see *5.6.5 JP1 Event converter*.

Example

```
{
  "pluginName":"PFMCS",
  "exceedJp1eventMaxDetected":false
  "events":[
    {
    "eventId":"2FFF",
    "message":"xxxxx",
    "attrs":{"SEVERITY":"Error","JP1_SOURCEHOST":"HOSTB"}
    },
    ...
  ]
}
```

(6) __createLink method

Description

The method generates a relation between retrieved configurations and returns it in JSON format.

- If the relation between retrieved configurations is generated successfully

  In the `__createLink` method, call the `addResult` (relation information between the retrieved configurations in JSON format) method.

- If the configuration information could not be retrieved

  Call the `args.setError` (error message) method, instead of the `addResult` method.

Make sure you call either the `addResult` or `args.setError` method.

The `__createLink` method is called within the `jddcreatetree` command that creates the system management tree of the Intelligent Integrated Management Base.

Parameters

The following table lists and describes the parameters of the `__createLink` method.

Table 4–23: Parameters of the __createLink method

No.	Member	Description	Remarks
1	`jp1UserName`	The JP1 user name	None
2	`jp1Token`	A JP1 authentication token that corresponds to `jp1UserName`	
3	`simtFileList`	List-formatted data of all configuration information	It contains multiple IM management node objects as its data structure.
4	`addResult(String json)`	The method to set the relation information between the retrieved configurations in JSON format	None
5	`setError(String message)`	The method for error notification. It sets an error code and a message.	

Format of relation information to be returned

The following describes the format of relation information between retrieved configurations returned by the `__createLink` method.

Formats

Format of the configuration information set for `setResult`:

```
{
"meta":{
    "format":"file-type",
    "componentName":"name-of-the-component-whose-relation-information-i
s-to-be-retrieved",
    "timestamp":"generation-time-of-relation-information"
    },
    "links":[
        {
        "from":"SID-of-the-preceding-node",
        "to":"SID-of-the-succeeding-node",
        "type":"type-of-operation-target",
        "value":structured-identifier
     }, ...
  ],
}
```

Describe

The following table lists and describes the items of relation information between the retrieved configurations.

Table 4–24: Items to describe the relation information between the retrieved configurations

No.	Item	Data type	Description
1	`meta`	array	Array that stores the data of the file

No.	Item	Data type	Description
2	format	string	The file format Always set this to conf. This attribute cannot be omitted.
3	componentName	string	Name of the component whose relation information is to be retrieved This attribute cannot be omitted.
4	timestamp	string	Returns the date and time of file creation as the UTC time in ISO8601 format. This attribute cannot be omitted. The time is the server time of JP1/IM - Manager that generated the relation information.
5	links	array	Array for relation information between configurations. The order of the array is irrelevant. If multiple pieces of relation information with the same from, to, and type values are found, these values are output with the jddcreatetree command, but the last relation information that appeared takes effect if the jddupdatetree is used to apply the information to the system. However, if the configuration information is from a JP1/AJS plug-in (componentName is /HITACHI/JP1/AJS3/CONFINFO) and type is rootJobnetExecutionOrder (root jobnet execution order) and from and to have the same value, the Intelligent Integrated Management Base merges objects stored in the value.unit array into a single link object and outputs it as an IM management node link file.
6	from	string	Preceding node. It specifies the SID of the preceding node. Example _ToolA-M_hostA/_HOST_hostA If the to attribute is specified, this attribute can be omitted. It cannot accept any control character.
7	to	string	Succeeding node. It specifies the SID of the succeeding node. Example _ToolA-M_hostA/_ToolA-A_hostB/_HOST_hostB If the from attribute is specified, this attribute can be omitted. It cannot accept any control character.
8	type	string	Specifies the type of relation information. It cannot accept a string starting with an underscore (_) or any control characters. Alphanumeric characters are available. The maximum number of characters is 255 bytes. type describes a grouping of relations that have the same meaning. On the **Related node** tab in the Integrated Operation Viewer window, you can filter relations to display only those belonging to a specific type. For relations within a JP1/IM product or between a JP1/IM product and another product, the following types are used. In addition to these types, the use of user-specified types is also allowed. • rootJobnetExecutionOrder: Relation of the execution order of root jobnets • rootJobnetAgent: Relation between a root jobnet and an AJS agent • managerAgent: Relation between the manager and agent of a JP1 product

No.	Item	Data type	Description
			• `sameNode`: Relation between nodes with the same name • `L2Connection`: Relation between layer-2 connection lines managed by JP1/NNMi • `Infrastructure`: Relation between infrastructure resources managed by JP1/OA • `monitoringConfiguration`: Relation between a product and a monitoring target in a monitoring product configuration The user can also specify any type in addition to this type.
9	`value`	Object	Specifies additional information for relation information between configurations. The following shows parameters supported by default when `type` is `rootJobnetAgent`: • `precedingJob`: Specifies the preceding job of a linked job by its full name. • `succeedingJob`: Specifies the succeeding job of a linked job by its full name. This attribute can be omitted.

Example

The following shows an example of retrieving information with the `__createLink` method.

```
{
  "meta":{
      "format":"conf"
      "componentName":"/HITACHI/JP1/AJS3/CONFINFO"
      "timestamp":"2018-11-11T00:00:00Z"
  },
  "links":[
      {
          "from":"JP1AJS-M_AJSM1/_HOST_AJShost1/_JP1SCHE_S1/_JP1JOBG_JG1/_
JP1ROOTJOBNET_root1",
          "to":"JP1AJS-M_AJSM2/_HOST_AJShost2/_JP1SCHE_S2/_JP1JOBG_JG2/_JP
1ROOTJOBNET_root2",
          "type":"rootJobnetExecutionOrder",
          "value":
             {
                       "precedingJob":"root1/job1",
                       "succeedingJob":"root2/job2",
             }
      }, ...
  ],
}
```

Impact of relation information set by addResult

The following table lists and describes the functions that are affected by the relation information set by `addResult` and its impact.

Table 4–25: List of affected functions

No.	Function	Impact
1	System status monitoring	The IM management node acquisition function outputs the IM management node link object as an IM management node link file.
2	Integrated monitoring of systems by IM management nodes	Relations are displayed in the **Workflow** tab according to IM management node links with `type` of `rootJobnetExecutionOrder` (root jobnet execution order).

No.	Function	Impact
3	Related node display	Relations are displayed in the **Related node** tab according to IM management node links.
4	Linked unit display	If an IM management node link has a `type` of `rootJobnetExecutionOrder` (root jobnet execution order), the unit information (including the result of `__linkValueGet`) specified for `unit` of the link's additional information (`value`) is displayed.
5	Display of impact on following root jobnets	If an IM management node link has a `type` of `rootJobnetExecutionOrder` (root jobnet execution order), the impact (result of `__linkValueGet`) of the unit (latest generation) specified for `unit` of the link's additional information (`value`) on following units is displayed.

(7) __linkValueGet method

Description

A method that adds dynamic grant information to the value parameter and returns an array of link information in the given JSON format.

If the plugin contains link information that cannot be processed, the link information will be returned as is.

Parameters

The following table lists and describes the parameters of the __linkValueGet method.

Table 4–26: Parameters of the __linkValueGet method

<table>
<tr><th>No.</th><th colspan="3">Member</th><th>Description</th><th>Remarks</th></tr>
<tr><td>1</td><td colspan="3"><code>jp1UserName</code></td><td>The JP1 user name</td><td rowspan="3">None</td></tr>
<tr><td>2</td><td colspan="3"><code>jp1Token</code></td><td>A JP1 authentication token that corresponds to <code>jp1UserName</code></td></tr>
<tr><td>3</td><td colspan="3"><code>linksData</code></td><td>An object for a link information object array</td></tr>
<tr><td>4</td><td rowspan="5"></td><td colspan="2"><code>links</code></td><td>An array of link information objects</td><td>It cannot be omitted. An empty array cannot be specified.</td></tr>
<tr><td>5</td><td rowspan="4"></td><td><code>from</code></td><td>SID of the preceding node</td><td rowspan="4">None</td></tr>
<tr><td>6</td><td><code>to</code></td><td>SID of the succeeding node</td></tr>
<tr><td>7</td><td><code>type</code></td><td>Type of the target</td></tr>
<tr><td>8</td><td><code>value</code></td><td>structured identifier</td></tr>
<tr><td>9</td><td colspan="3"><code>select</code></td><td>An array of <code>value</code> parameters to be retrieved.
If you want to further specify an object or a member of an object array, specify <i>object-name</i><code>.</code><i>member-name</i>.
If you want to specify only <code>"impact"</code> in the following example, specify <code>"unit.impact"</code> in <code>select</code>:<pre>"value":{
    "unit": [
        {
           "precedingJob":"job1
",
           "succeedingJob":"job
2"
           "impact":true
        }</pre></td><td>It can be omitted.
If omitted, it retrieves all the parameters.</td></tr>
</table>

No.	Member	Description	Remarks
		] }	
10	`setResult(String json)`	The method to set link information in JSON format	None
11	`setError(String message)`	The method for error notification. It sets an error message.	

Format of link information to be returned

The following describes the format of link information returned by the `__linkValueGet` method.

Formats

```
{
   "links": [
      {
          "from": "the-preceding-node-SID",
          "to": "the-succeeding-node-SID",
          "type": "type-of-the-target",
          "value": structured-identifier
       },  ...
  ]
}
```

Describe

The following table lists and describes the items of retrieved link information.

Table 4–27: Items of the retrieved link information

No.	Item	Data types	Description
1	`links`	array	An array of link information
2	`from`	string	SID of the preceding node
3	`to`	string	SID of the succeeding node
4	`type`	string	Type of the target
5	`value`	Object	Specifies additional information of relation information between configurations.

Example

The following shows an example of retrieving information with the `__linkValueGet` method.

```
{
   "links": [
      {
         "from":"_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv/_JP1JO
BG_jobgroup/_JP1ROOTJOBNET_jobnet1",
         "to":"_JP1AJS-M_HOST1/_HOST_HOST1/_JP1SCHE_schedulerserv/_JP1JOBG
_jobgroup/_JP1ROOTJOBNET_jobnet2",
         "type":"rootJobnetExecutionOrder",
         "value":{
              "unit": [
                   {
                     "precedingJob":"job1",
                     "succeedingJob":"job2"
                     "succeedingJobStartTime":"2019-05-14T00:00:00Z",
                     "precedingJobURL":"http://10.220.196.82:22252/ajs/...
",
                     "succeedingJobURL":"http://10.220.196.82:22252/ajs/..
.",
                     "impact":"error"
                   }   ...
               ],
               "msg":"KAJY04254-E The collecting information process coul
d not be generated."
           }
      }, ...
  ]
}
```

Impact of additional information (value) of a link set by setResult

The following table lists and describes the functions that are affected by the additional information (`value`) of a link set by `setResult` and its impact.

Table 4–28: List of affected functions

No.	Function	Impact
1	Linked unit display	If an IM management node link has a `type` of `rootJobnetExecutionOrder` (root jobnet execution order), the information specified for `unit` of the link's additional information (`value`) is displayed. In addition, the URL parameter is used to start the WWW browser on which the URL is specified.
2	Display of impact on following root jobnets	If an IM management node link has a `type` of `rootJobnetExecutionOrder` (root jobnet execution order), the impact of the unit (latest generation) specified for `unit` of the link's additional information (`value`) on following units is displayed.

(8) __simtLoad method

Description

This method is called to collect the required related information when IM management node is loaded. Called from simt service when the managed node is updated with the following actions:

- When simtData loading is completed at service startup
- When simtData loading is completed when the jddupdatetree command is executed

Collected information can be provided to other methods, for example, by setting the information to a global variable. For example, if the __simtLoad method collects AJS manager host name and AJS Agent host and set it global variable, you can refer to it in other methods (__eventGet method).

- When related information retrieval is completed normally

  You can provide information about other methods, for example by setting the global variable.
- Failed to get related information

  Ensure that you call args.setError (error message) method.

Parameters

The following table lists and describes the parameters of the `__simtLoad` method.

No.	Member	Description	Remarks
1	`simtDataList`	All itemized lists of configuration simtData	All simtData in the master information of the managed node
2	`setError(String message)`	Methods for error notifications Set the error code and Message.	None

(9) __metricListGet method

Description

The method retrieves the list of metrics that can be displayed for time-series data and returns it in JSON format.

Parameters

The following table lists and describes the parameters of the __metricListGet method.

Table 4–29: Parameters of the __metricListGet method

No.	Member	Description	Remarks
1	`jp1UserName`	The JP1 user name	None
2	`jp1Token`	A JP1 authentication token that corresponds to `jp1UserName`	
3	`sid`	A configuration information SID whose list of metrics you want to retrieve	
4	`lang`	Language for the list of metrics to be retrieved	
5	`setResult (String json)`	The method to set the list of metrics retrieved in JSON format	
6	`setError (String message)`	The method for error notification. It sets an error message.	

Format of the list of metrics to be returned

The following shows the list of metrics returned by the `__metricListGet` method.

Formats

```
{
    "metrics":[
      {
         "name":"metric",
         "label":"metric-display-name",
         "category":"category-of-the-metric",
         "description":"description-of-the-metric",
         "default":default-setting
    }
  ...
]
```

Describe

The following table lists and describes the items of the retrieved list of metrics.

Table 4–30: Items of the retrieved list of metrics

No.	Item	Data types	Description
1	`metrics`	array	An array of metric information.

No.	Item	Data types	Description
			You can specify up to 100 elements. An empty array cannot be specified. This item cannot be omitted.
2	name	string	The name of the metric. It can be specified with half-width alphanumeric characters and the following symbols: - (hyphen), _ (underscore) It must be specified between 1 and 255 characters. An empty string cannot be specified. This item cannot be omitted.
3	label	string	The display name of the metric. It can be specified between 1 and 255 characters, excluding control characters. An empty string cannot be specified. This item can be omitted.
4	category	string	The category of the metric. It can be specified between 1 and 255 characters, excluding control characters. An empty string cannot be specified. This item can be omitted.
5	description	string	The description of the metric. It can be specified between 1 and 1023 characters, excluding control characters. An empty string cannot be specified. This item can be omitted. If a long string is specified in this item, when you use the Integrated Operation Viewer window of JP1/IM - Manager (Intelligent Integrated Management Base), a string displayed as a tooltip for the metric display name in the **Trends** tab might be truncated by WWW browser limitations (maximum number of characters that can be displayed as the title attribute).
6	default	boolean	Specifies whether the metric is a default metric. • true: It is a default metric. • false: It is not a default metric. You can specify up to 10 metrics as the default metrics. This item cannot be omitted.

Example

The following shows an example of retrieving information with the __metricListGet method.

```
{
    "metrics":[
      {
        "name":"CPU-Usage",
        "label":"CPU-used-rate",
        "category":"CPU",
        "description":"Show the CPU usage on a core basis. (Units: %)",
        "default":true
      }
     ...
    ]
}
```

Impact of the list of metrics set by setResult

The following table lists and describes the function that is affected by the list of metrics set by setResult and its impact.

Table 4–31: List of affected functions

No.	Function	Impact
1	Trend information display	In the trend graph settings area of the **Trends** tab, the metrics are displayed as candidates of metrics to be displayed in a chart.

(10) __timeSeriesDataGet method

Description

The method retrieves time-series data and returns it in JSON format.

If the number of time-series data sets retrieved and the number of instances exceed the limits specified by `countPerInstance` and `instanceCount` respectively, the applicable member of the `exceedCountDetected` object in the response is set to `true` and the data is selected so that the numbers of data sets are below the limits of `countPerInstance` and `instanceCount`, and then the data is returned.

Parameters

The following table lists and describes the parameters of the __timeSeriesDataGet method.

Table 4–32: Parameters of the __timeSeriesDataGet method

No.	Member	Description	Remarks
1	`jp1UserName`	The JP1 user name	None
2	`jp1Token`	A JP1 authentication token that corresponds to `jp1UserName`	
3	`sid`	A configuration information SID whose time-series data you want to retrieve	
4	`lang`	Language for time-series data to be retrieved	
5	`metric`	The name of the metric. It must be specified between 1 and 255 characters. An empty array cannot be specified. This item cannot be omitted.	
6	`startTime`	Specifies the start date and time of the time-series data as the UTC time in ISO8601 format. Do not specify seconds after the decimal point.	
7	`endTime`	Specifies the end date and time of the time-series data as the UTC time in ISO8601 format. Do not specify seconds after the decimal point.	
8	`countPerInstance`	The upper limit of the number of data sets per instance in those to be retrieved	It is ensured that a value obtained by multiplying the `countPerInstance` value by the `instanceCount` value is less than or equal to 30,000.
9	`instanceCount`	The upper limit of instances	
10	`setResult (String json)`	The method to set time-series data in JSON format	None
11	`setError (String message)`	The method for error notification. It sets an error message.	

Format of time-series data to be returned

The following shows the time-series data returned by the `__timeSeriesDataGet` method.

Formats

```
{
    "metric":"metric",
    "timeSeriesData":[
            {
               "instance":"instance-name"
               "unit":"unit",
               "data":[
               {"time":"time","value":value},
                   ...
            ]
          },
          ...
    ],
    "exceedCountDetected": {
        countPerInstance:whether-an-excess-of-the-upper-limit-for-the-n
umber-of-data-sets-per-instance-is-detected,
        instanceCount: whether-an-excess-of-the-upper-limit-for-the-num
ber-of-instances-is-detected
    }
}
```

Describe

The following table lists and describes the items of the retrieved time-series data.

Table 4–33: Items of the retrieved time-series data

No.	Item	Data types	Description
1	`timeSeriesData`	array	An array of time-series data. An empty array cannot be specified. This item cannot be omitted.
2	`metric`	string	The name of the metric. It can be specified with half-width alphanumeric characters and the following symbols: - (hyphen), _ (underscore) It must be specified between 1 and 255 characters. An empty string cannot be specified. This item cannot be omitted.
3	`instance`	string	The name of the instance. It can be specified between 1 and 255 characters, excluding control characters. An empty string cannot be specified. This item can be omitted.
4	`unit`	string	The unit for the metric. It can be specified between 1 and 255 characters, excluding control characters. An empty string cannot be specified. This item cannot be omitted.
5	`data`	array	An array of two-dimensional data consisting of the time and value. If no time-series data exists in the specified period, specify an empty array. This item cannot be omitted.
6	`time`	string	The time of data. It is the UTC time in ISO8601 format. The number of seconds after the decimal point cannot be specified. • If `data` is empty: This item can be omitted. • If `data` is not empty: This item cannot be omitted. An empty string cannot be specified.
7	`value`	number	A value of data. It should be the same as the accuracy of `number` in JavaScript. • If `data` is empty: This item can be omitted. • If `data` is not empty: This item cannot be omitted.
8	`exceedCountDetected`	Object	The object to detect the upper limit. This item cannot be omitted.
9	`countPerInstance`	boolean	Whether an excess of the upper limit for the number of data sets per instance is detected.

No.	Item	Data types	Description
			• If the upper limit is exceeded: `true` • Otherwise: `false` This item cannot be omitted.
10	`instanceCount`	boolean	Whether an excess of the upper limit for the number of instances is detected. • If the upper limit is exceeded: true • Otherwise: false This item cannot be omitted.

Example

The following shows an example of retrieving information with the `__timeSeriesDataGet` method.

```
{
    "metric":"CPU Usage",
    "timeSeriesData":[
            {
              "instance":"CPU_1"
              "unit":"%",
              "data":[
                  {"time":"2019-05-22T00:00:00Z","value":14.04},
                                  ...
              ]
          },
            {
              "instance":"CPU_2"
              "unit":"%",
              "data":[
                {"time":"2019-05-22T00:00:00Z","value":09.24},
                                  ...
            ]
          },
       ...
    ],
    "exceedCountDetected": {
        "countPerInstance": true,
        "instanceCount": false
    }

}
```

If no data exists for the specified metric and in the specified period

```
{
    "metric":"CPU Usage",
    "timeSeriesData":[
            {
              "unit":"%",
              "data":[
              ]
          }
    ],
    "exceedCountDetected": {
        "countPerInstance": false,
        "instanceCount": false
    }
}
```

Impact of the time-series data set by setResult

The following table lists and describes the function that is affected by the time-series data set by `setResult` and its impact.

Table 4–34: List of affected functions

No.	Function	Impact
1	Trend information display	The trend of time-series data is displayed.

(11) __urlGet method

Description

The method retrieves the URL for starting a monitor associated with the specified SID and returns it in JSON format.

Parameters

The following table lists and describes the parameters of the __urlGet method.

Table 4–35: Parameters of the __urlGet method

No.	Member	Description	Remarks
1	`jp1UserName`	The JP1 user name	None
2	`jp1Token`	A JP1 authentication token that corresponds to `jp1UserName`	
3	`sid`	A configuration information SID whose URL for starting the associated monitor you want to retrieve	
4	`setResult (String json)`	The method to set the URL information in JSON format	
5	`setError (String message)`	The method for error notification. It sets an error message.	

Format of the URL for starting the monitor to be returned

The following shows the URL for starting the monitor returned by the `__urlGet` method.

Formats

```
{
    urlList:[
        {
            "url":"URL-for-starting-the-monitor",
            "name":"name-of-the-URL"
        },
        ...
    ]
}
```

Describe

The following table lists and describes the items of the retrieved URL for starting the monitor.

Table 4–36: The items of the retrieved URL for starting the monitor

No.	Item	Data types	Description
1	`urlList`	array	An array of URL information objects

No.	Item	Data types	Description
2	`url`	string	The URL string
3	`name`	string	The name of the URL

Example

The following shows an example of retrieving information with the `__urlGet` method.

```
{
    urlList:[
       {
            "url":"http://10.220.196.82:22252/ajs/login.html?manager=10.22
0.196.82&type=monitor...",
            "name":"monitor-startup-window-for-rootJobNet1"
       }
    ]
}
```

Impact of the URL information set by setResult

The following table lists and describes the function that is affected by the URL information for starting the monitor set by `setResult` and its impact.

Table 4–37: List of affected functions

No.	Function	Impact
1	Opening a window of a linked product	A window of a linked product is opened for the IM management node with `__urlGet` specified for `methods` of additional information (`value`) in the configuration information.

4.4.5 Exception handling

If an exception occurs in a method of the user-created plug-in, it should be caught (`catch`) within that method. If an exception occurs in a method of the plug-in, set the error and message that correspond to the exception to the argument of the error message method (`args.setError`) and then call the method. Use English for the language of the error message you set.

Note that after the error message method (`args.setError`) is called, the plug-in will never get the control back.

The following message is printed to the integrated trace log or window:

```
KAJY02028-W An attempt to acquire the system configuration information that
manages JP1/IM - Manager has failed. (Host name: host-name, Component name:
component-name, Details: details)
```

host-name

The name of the host from which information could not be retrieved

component-name

The name of the component from which information could not be retrieved

details

The contents of the message returned by the `setError` method

For details on the error message method (`args.setError`), see *4.4.4(1) __configurationGet method* in *4.4 Methods implemented in the plug-in*.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

4.5 Methods available in the user-created plug-in

The following table lists and describes the methods that are commonly available in the methods of the user-created plug-in.

Table 4–38: List of methods commonly available in the methods of the user-created plug-in

No.	Method name#	Description
1	`jp1Imdd.callRest`	The method to call the REST API
2	`jp1Imdd.readFile`	The method to read a file and return the content of the file as a string
3	`jp1Imdd.encodeBase64`	The method to convert a string into a Base64-formatted value and return it
4	`jp1SimtService.get`	The method to return the configuration information SID and the data labeled `value`
5	`jp1SimtService.join`	The method to return the configuration information SID that has been generated by combining structured identifiers
6	`jp1SimtService.pack`	The method to return the structured identifier generated by combining the class and name of the structured identifier that takes a non-host-name value for the name
7	`jp1SimtService.packHost`	The method to return the structured identifier generated by combining the class and name of the structured identifier that takes a host name for the name
8	`jp1SimtService.parse`	The method to split a configuration information SID into structured identifiers, separate each structured identifier into the class part and the URL-decoded name part with the underscore (_) between them removed, and return the resulting data
9	`jp1Logger.trace`	The method for logging
10	`jp1Imdd.execCmd`	The method to execute a command remotely
11	`jp1Imdd.getPluginConfDirPath`	The method to return the absolute path to the parent directory of the directory that stores plug-in definition files
12	`jp1Imdd.getVersion`	The method to return the version of JP1/IM
13	`jp1EmService.getEvent`	The method to retrieve events related to an IM management node from the integrated monitoring database
14	`jp1SimtService.getLink`	The method to retrieve link information
15	`jp1EmService.changeEventStatus`	The method to change the event status
16	`jp1SimtService.getTreeSid`	The method to retrieve the tree SID corresponding to the specified configuration information SID
17	`jp1TrendDataService.getTrendData`	Methods that retrieve trend data (time-series data) from Trend data Management Database
18	`jp1TrendDataService.getLabelList`	A method that retrieves a list of time series of label sets from Trend data Management Database that Match to a parameter-specified condition.

#

`jp1Imdd`, `jp1SimtService`, and `jp1Logger` of these methods represent a global object. So, do not define a global object with the same name as one of these names. Also, do not define a global object with the name that starts with `jp1` or `hitachi`.

4.5.1 jp1Imdd.callRest

This method calls a REST API. The following table shows the details of the `jp1Imdd.callRest` method.

Method name

```
Object jp1Imdd.callRest(String method, String url, Object headers,
String body)
```

Parameters

`method`

A method of a REST API

`url`

The URL of the REST API

When the URL including host name is specified, register the host name to the integrated manager's hosts file and DNS so as to enable name resolution on the integrated manager host. Configuration in `jp1hosts` file and `jp1hosts2` file are not referred.

`_headers`

The request header of the REST API

`body`

The request body of the REST API

If the `GET` method is specified and the body is not needed, set `body` to null or an empty character.

Return values

An object that stores the response from the REST API.

The object contains the following keys and values:

No.	Description		Key	Value
1	If the REST API is completed successfully		`"response"`	response object
		Keys and values that are stored in the response object	`"status"`	HTTP status code
			`"headers"`	response header
			`"body"`	response body
2	If the analysis of the URI fails		`"error"`	error object
		Keys and values that are stored in the error object	`"status"`	`0`
			`"body"`	string indicating an analysis error
3	If the HTTP status code is 4*xx* or 5*xx*, or an unknown status code is returned		`"error"`	error object
		Keys and values that are stored in the error object	`"status"`	HTTP status code
			`"headers"`	response header
			`"body"`	response body

Exception

`RestClientException`

- When an I/O error occurs

Call example

```
module.exports = function(args) {
    var baseUrl = args.baseUrl;
    var manager = args.manager;
    var jp1token = args.jp1token;

    var method = 'POST';
    var apiPath = '/v1/authorization/token';
    var url = baseUrl + apiPath;
    var headers = {
        'Accept': 'application/json',
        'Content-Type': 'application/json',
        'X-AJS-Authorization-Token': jp1token,
    };
    var body = {
        parameters: {
            manager: manager,
            serviceName: 'AJSROOT1',
        }
    };
    return jp1Imdd.callRest(method, url, headers, JSON.stringify(body));
}
```

4.5.2 jp1Imdd.readFile

This method reads a file located at the path specified by the parameter and returns its content as string type. This method can read a UTF-8 encoded file. The following table shows the details of the `jp1Imdd.readFile` method.

Method name

`String jp1Imdd.readFile(String pathname)`

Parameters

`pathname`

The absolute path to the file to be read by the method.

Separate the path with a forward slash (/) or backslash (\).

Return values

The content of the file the method read

If a BOM is placed in the file, a string without the BOM is returned.

Exception

`FileNotFoundException`

- The file cannot be opened for some reasons
- If the file does not exist, the file is not a normal file but a directory

`IOEXception`

- If an I/O error occurs

4.5.3 jp1Imdd.encodeBase64

This method encodes a string specified by the parameter in Base64 format and returns it as string type. The following table shows the details of the `jp1Imdd.encodeBase64` method.

Method name

`String jp1Imdd.encodeBase64(String str)`

Parameters

`str`

String to be Base64-encoded

Return values

Base64-encoded string

Exception

None

4.5.4 jp1SimtService.get

Based on the configuration information SID specified in its parameter, this method returns the `SimtData` object that puts together the SID in question and the data labeled `value`. The following table shows the details of the `jp1SimtService.get` method.

Method name

`SimtData jp1SimtService.get(String sid)`

Parameters

`sid`

String representing the configuration information SID

Return values

`SimData` object that puts together the configuration information SID and the data labeled `value`

If the configuration information SID specified in the parameter does not exist, this method returns null.

The `SimtData` object has the following fields:

- `String sid`
- `Map<String, Object> value`

Exception

None

4.5.5 jp1SimtService.join

This method generates a configuration information SID by combining the structured identifiers specified in its parameter by inserting a slash (`/`) between them, and returns the generated configuration information SID in string format. The following table shows the details of the `jp1SimtService.join` method.

Method name

`String jp1SimtService.join(String... sid)`

Parameters

`sid`

Structured identifiers that are combined using slash (`/`)

Return values

String representing the configuration information SID that consists of multiple strings representing the structured identifiers specified in the parameter, combined with a slash (`/`)

Exception

None

4.5.6 jp1SimtService.pack

This method encloses the class (without underscores) in the structured identifier specified by the first parameter with underscores (_), URL-encodes symbols other than `.`, ~, `-`, and `:`, and non-alphanumeric characters in the name specified by the second parameter, concatenates the class with the name in this order, and then returns the generated structured identifier as string type. The following table shows the details of the `jp1SimtService.pack` method.

Method name

```
String jp1SimtService.pack(String key, String value)
```

Parameters

`key`

The class in the structured identifier that is to be enclosed with underscores (_)

Class in the structured identifier that takes a non-host-name value for the name

`value`

The name in the structured identifier to be URL-encoded

Return values

A structured identifier string created by combining the class string enclosed by underscores (_) with the URL-encoded name string

Exception

None

4.5.7 jp1SimtService.packHost

This method encloses the class (without underscores), for which the name of the structured identifier accepts a host name, in the structured identifier specified by the first parameter with underscores (_). Then, the method converts the host name specified by the second parameter into uppercase characters and URL-encodes symbols other than `.`, ~, `-`, and `:`, and non-alphanumeric characters, concatenates the class with the name in this order, and then returns the generated structured identifier as string type. If you create a structured identifier that has a non-host-name value for the name, use the `jp1SimtService.pack` method. The following table shows the details of the `jp1SimtService.packHost` method.

Method name

```
String jp1SimtService.pack(String key, String value)
```

Parameters

`key`

The class in the structured identifier that is to be enclosed with underscores (_)

Class in the structured identifier that takes a non-host-name value for the name

`value`

The host name that is converted into uppercase characters and URL-encoded

Return values

A structured identifier string created by combining the class string enclosed by underscores (_) with the URL-encoded name string

Exception

None

4.5.8 jp1SimtService.parse

This method splits the SID specified by the parameter into structured identifiers and separates the identifiers into classes without underscores (_) and URL-decoded names. The method then stores these pairs of classes and names in `SimtIdUnit` objects and returns a `List` that contains the `SimtIdUnit` objects. If the SID is split into structured identifiers but these identifiers are not in the valid structured identifier format, such identifiers are stored in the `SimtIdUnit` object as name values. The following table shows the details of the `jp1SimtService.parse` method.

Method name

```
List<SimtIdUnit> jp1SimtService.parse(String sid)
```

Parameters

`sid`

String that represents the SID

Return values

A `List` object that contains `SimtIdUnit` objects storing the class obtained by splitting the SID into structured identifiers and removing underscores (_) from it, together with the URL-decoded name

The `SimtIdUnit` object has the following fields:

- `String key`: Class without underscores
- `String value`: Name

Exception

None

4.5.9 jp1Logger.trace

This method writes the string in the second parameter to the file specified by the first parameter as a log. The following table shows the details of the `jp1Logger.trace` method.

Method name

```
void jp1Logger.trace(String jsName, String message)
```

Parameters

`jsName`

Specify the file name of the user-created plug-in for the file name parameter. The logs are output to the location where the user-created plug-in is located. A single row can contain up to 4,096 bytes. If the log exceeds the upper limit, the portion beyond the limit is not written to the file.

`message`

The output message

Return values

None

Exception

None

4.5.10 jp1Imdd.execCmd

This method executes a command specified in the parameter. The following table shows the details of the `jp1Imdd.execCmd` method.

Method name

`Object jp1Imdd.execCmd(String host, String cmd, Object env, String envFile, String jp1user)`

Parameters

If the file specified by `envFile` also contains the environment variable specified by `env`, the value specified by `env` takes precedence.

`host`

Specifies the name of the command execution host from 1 to 255 bytes.

`cmd`

Specifies the command to be executed and its arguments from 1 to 4,095 bytes. If the command name contains any space character, it must be enclosed in double quotation marks (`"`).

`env`

Specifies the environment variable value for the value of the object, using the environment variable when the command is executed on the execution host as a key to the object. Up to 30 env parameters can be specified.

If it is not needed, specify null. Specify both the object key and value together from 1 to 7,107 bytes.

`envFile`

The name of the environment variable file. Specify the absolute path to the file on the execution host between 1 and 255 bytes. If it is not needed, specify null or an empty string.

`jp1user`

Specifies a JP1 user name from 1 to 31 bytes. If the value is specified, the command is executed as the primary user of the specified JP1 user. If it is not needed, specify null or an empty string.

Return values

An object that stores the execution result of the command. The object contains the following keys and values:

No	Description	Key	Value
1	If the command is executed remotely and successfully (the executed command is started successfully)#	`"response"`	response object
	Keys and values that are stored in the response object	`"rc"`	Return value of the executed command
		`"stdOut"`	String of the standard output of the command, converted into UTF-8
		`"stdError"`	String of the standard error output of the command, converted into UTF-8
2	If the remote execution of the command fails (the executed command cannot be started successfully)	`"error"`	error object
	Keys and values that are stored in the error object	`"rc"`	error code

#:

Even if the execution command specified in `cmd` does not exist, if the connection to the execution host is successfully established and `cmd.exe` or `/bin/sh` starts up, the return value, standard output, and standard error output are returned. Furthermore, the return value, standard output, and standard error output that are returned depend on the `cmd.exe` or `/bin/sh` of the execution host.

Exception

`IOEXception`

- When an I/O error occurs

Prerequisite

To use this method, JP1/Base 12-10 or later must be installed in the execution host and added to IM configuration management.

Commands that can be executed

The following shows the types of commands that can be executed by the `jp1Imdd.execCmd` command.

If a command is executed on a Windows host:

- Executable file (`.com`, `.exe`)
- Batch fil (.bat)

If a command is executed on a UNIX host:

- UNIX command
- Shell script

> **Important**
>
> If a command is executed, it works assuming that the language setting is the same as the one with which JP1/Base is running. Do not change characters with the `LANG` environment variable.

The following commands cannot be executed:

- Command that needs interactive operations
- Command that opens a window
- Command that involves escape sequences and control codes
- Command that does not exit, such as a daemon

- Command that needs interactions with the desktop, such as the Windows messaging mechanism and DDE (In Windows)
- Command that shuts down the OS, such as `shutdown` and `halt`
- Command that exits JP1/Base
- `jbs_spmd_reload` command

How to execute a command

The remote command execution function executes a command with the following operations.

In Windows:

```
cmd.exe /c specified-command
```

InUNIX:

The login shell of the OS user is used. If it is not specified, `/bin/sh` is used.

```
/bin/sh -c specified-command
```

Execution user

The command is executed as the primary user of the JP1 user specified in the `jp1User` argument. If `jp1User` is set to null or an empty string, the command is executed with the following privilege of the execution host.

- In Windows: `SYSTEM`
- In UNIX: `root`

Important

If UAC is enabled on the execution host, the primary user of the JP1 user specified by the `jp1User` argument must be the built-in Administrator user.

Limits

The following table describes the limits that apply to jp1Imdd.execCmd method.

Table 4–39: Limitations to jp1Imdd.execCmd method

No.	item	Value to be specified
1	Time out (second)	3600
2	Size of the standard output and standard error output (MB)	20

Error code

The following table shows the error codes when the execution target command fails to be started.

Table 4–40: Error codes when the execution target command fails to be started

No.	Error case	Error code	Status
1	The specified parameter is invalid	1	Revise the specified parameter and re-execute the command.
2	A connection to the execution host failed	2	Check to see if the JP1/Base service is running on the execution host.
3	A timeout occurred#	3	A timeout occurred due to a high load on the execution host or the network. Wait a while and then re-execute the command.

No.	Error case	Error code	Status
4	The amount of incoming data exceeded its upper limit	4	The size of the standard output or the standard error output for the executed command exceeded its upper limit. Revise the output of the executed command.
5	The environment variable file cannot be read	5	Check to see if the file specified by the `envFile` argument exists on the execution host.
6	The JP1 user is invalid	6	Check the JP1 user specified by the `jp1User` argument to see if: • The user is mapped with the OS user on the execution host. • The server hosts with user mapping contain the JP1/IM hosts.
7	Internal error	255	Use the data collection tool to collect data and contact the system administrator.

#:

When a timeout occurs, the process of the command currently running is terminated.

Note

If UAC is enabled on the execution host, the primary user of the JP1 user specified for `jp1User` must be the built-in Administrator user.

4.5.11 jp1Imdd.getPluginConfDirPath

This method returns the absolute path to the parent directory of the directory that stores plug-in definition files as string type. The following table shows the details of the `jp1Imdd.getPluginConfDirPath` method.

Method name

`String jp1Imdd.getPluginConfDirPath (pluginName)`

Parameters

`pluginName`

String that indicates the name of the plug-in

Example: `jp1pfm`

Return values

The method returns a string representing the absolute path to the directory under which the plug-in definition files are stored.

When null is specified in the parameter or in the event of an internal error, null is returned.

Example: In physical hosts of Windows.

```
Manager-path\conf\imdd\plugin\jp1pfm
```

Exception

None

4.5.12 jp1Imdd.getVersion

This method returns the version of JP1/IM as string type. The following table shows the details of the `jp1Imdd.getVersion` method.

Method name

String jp1Imdd.getVersion ()

Parameters

None

Return values

Returns the version of the product in *VV*-*RR* or *VV*-*RR*-*SS* format.

For example, the returned value is 12-00 which omits SS when the version of the product is 12-00, and the returned value is 12-00-02 when the version of the product is 12-00-02.

The method returns the same value as productVersion of the version information acquisition API. For details, see *5.12.1 Version information acquisition*.

Exception

None

Example

To make a user-created plug-in downward compatible, check the version of JP1/IM as shown below to branch out the process.

```
var im2Version = null;

if(typeof jp1Imdd.getVersion == "function") {
    im2Version = jp1Imdd.getVersion();
} else {
    im2Version = "12-00";
}

switch(im2Version) {
    case "12-00":
        // Operations for 12-00
        break;
    case "12-10":
       // Operations for 12-10
        break;
}
```

4.5.13 jp1EmService.getEvent

This method retrieves events related to an IM management node from the integrated monitoring database. Specifically, a list of events matching the conditions specified by the parameters is retrieved.

If the JP1 user who specified this method does not have the permission to view the events in question, the user cannot retrieve them. In this case, no error message is output.

The range of events that can be retrieved depends on the JP1 resource group settings and the event receiver filter settings in JP1/IM - Manager. For details about the conditions under which a user may be able to view certain events, see information regarding the events that can be displayed in the event view when an IM management node is selected in *3.5.1 Structure of the IM management node* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This method cannot be called from the __eventGet method provided by product plug-ins or from the method called by the __eventGet method.

The details of the `jp1EmService.getEvent` method are provided below.

Method name

```
Object jp1EmService.getEvent(String sid, Object filter, String direction,
String since, int count, String[] attrs, int[] statusFilter, boolean
consolidateEvent, int searchCount, String lang, String jp1User,
String jp1Token)
```

Parameters

`sid`

Specify the tree SID of an IM management node. A list of events issued by the specified IM management node is retrieved.

If you specify `null` or an empty string, it is assumed that all systems (`_ROOT_AllSystems`) are specified. If you specify `null` or an empty string without any IM management nodes having been set up, an empty list of events is returned.

`filter`

Specify an event search condition object.

This method searches the integrated monitoring database for events that meet the specified event search conditions. For details about the event search condition object, see *7.2.1 (3) Event search condition object*. If you specify a single-byte space as any of the attribute values, it is assumed that `%20` is specified.

You can narrow down the events specified with `sid` to those that meet the event search conditions specified with `filter`. If you do not need to narrow down the retrieved events, specify `null` for `filter`.

When there is no pass-conditions group that contains both an event search condition in which `key` is set to `B.TIME` (registered time) and `ope` is set to `TRANGE` (time) and an event search condition in which `key` is set to `B.ARRIVEDTIME` (arrived time) and `ope` is set to `TRANGE` (time)[#], it is assumed that one of the pass-conditions groups is specified as follows:

```
{"key":"B.TIME","ope":"TRANGE","val":["1-day-before-current-time","curr
ent-time"]}
```

#: This includes specifying `null` for `filter`.

In an event search condition in which `key` is set to `B.ID` (event ID), the digits of the value specified for `val` are automatically padded with zeros.

`direction`

Specify the direction in which to search for events.

Specify `past` to search for events that occurred before the specified event and `future` to search for events that occurred after the specified event. If you specify `null` or an empty string, it is assumed that `past` is specified.

`since`

Specify the SID of the JP1 event that serves as a starting point for the event search. The method searches for events that occurred either before or after the JP1 event corresponding to the specified SID. Note that the JP1 event corresponding to the specified SID is not included in the search. If you specify `null` or an empty string, the integrated monitoring database is searched from either the beginning or end depending on the setting specified for `direction`. For details about the SIDs of JP1 events, see *7.2.1 (1) Event information object*.

`count`

Specify the maximum number of events to be retrieved in the range from 1 to 2,000.

`attrs`

Specify an array of event attributes to be retrieved.

Example:

```
"attrs":["B.ID","B.MESSAGE",...]
```

The attributes specified for attrs are retrieved in user-specified order. When null is specified, attributes are acquired differently depending on the type of JP1 events specified.

- When consolidation start events are specified

  All the attribute values that can be output by the event report output function are retrieved first. Afterwards, the attributes listed in the table under *Event attributes of the consolidation start event* in *7.2.1 (1) Event information object* are retrieved.

- When events other than consolidation start events are specified

  All the attribute values that can be output by the event report output function are retrieved. The specifiable event attributes include all the attributes that can be output by the event report output function and the attributes listed in the table under *Event attributes of the consolidation start event* in *7.2.1 (1) Event information object*.

For details about the event report output function, see *4.15.2 Saving event information in the integrated monitoring database (CSV report)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

statusFilter

To narrow down the events to those whose nodes match the specified status, specify status values by using the int array.

Example: To retrieve only those events whose node status is 30 and 40

```
"statusFilter":[30,40]
```

For details about the node status codes, see *5.8.5 IM management node status acquisition*. If you do not need to narrow down events, specify null.

consolidateEvent

When repeated events have been consolidated on the Intelligent Integrated Management Base, specify whether you want the consolidated repeated events to be returned. To prevent repeated events from being returned, specify true.

- true

  When the display of repeated events is suppressed on the Intelligent Integrated Management Base, only the consolidation start events are returned. Repeated events that come after each consolidation start event are not returned.

- false

  Repeated events are returned regardless of whether the display of repeated events is suppressed on the Intelligent Integrated Management Base.

searchCount

Specify the maximum number of times a search for events can be repeated in the range from 0 to 120,000.

A total of 100 events mapped to the IM management node specified by the sid parameter are searched through, starting from the event specified by the since parameter and proceeding in the direction specified by the direction parameter.

When the number of events specified by the count parameter cannot be retrieved due to an event receiver filter or other restrictions, the search is repeated, that is, the next 100 events are searched through. The maximum number of times the search for events can be repeated is what you need to specify for this parameter.

When the specified maximum limit is reached, the search is discontinued, and a list of all events retrieved before the discontinuation of the search is output along with the KAJY32010-W message. If you specify nothing or 0 for this parameter, there is no limit to the number of times a search can be repeated.

lang

Specify the language of the message. You can specify ja, ja-JP, or en. If you specify any other values, it is assumed that en is specified. For details, see *Language conventions of user-created plug-ins* in *4.4 Methods implemented in the plug-in*.

jp1User

By using a string of 1 to 31 bytes, specify the name of a JP1 user who has one of the following JP1 permission levels. Only the events that the specified JP1 user has the permission to view are retrieved.

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

jp1Token

Specify a JP1 authentication token for the JP1 user specified for jp1User.

Return values

After successful retrieval of events, an object storing event information is returned. The following table describes the keys and their values stored in the object after successful retrieval of events:

No.	Key	Value
1	eventData	Returns an array of event information objects that represents a list of retrieved events. For details about event information objects, see *7.2.1 (1) Event information object*. When there is no event to be returned, a zero-length array is returned.
2	messageId	Returns the message ID of a temporary error message generated during an event search. Either KAJY32005-W or KAJY32010-W is returned. When there is no message to be provided, null is specified. For details about messages, see the *JP1/Integrated Management 3 - Manager Messages*.
3	message	Returns the body of a temporary error message generated during an event search. When there is no message to be provided, null is specified.
4	beginSid	Returns the SID of a JP1 event that is right next to (that is, immediately before or after, depending on the specified direction of event search) the event that has been specified by the since parameter as the starting point for the event search. When there are no JP1 events to be searched for, this key is omitted.
5	endSid	Returns the SID of the JP1 event located at the end position of the event search. When the event search is discontinued, the SID of the JP1 event where the search was discontinued is returned. When there are no JP1 events to be searched for, this key is omitted.

The following table describes the keys and their values stored in the object after a failed attempt to retrieve events:

No.	Key	Value
1	errorMessage	An error message. When any of the arguments are invalid, the KAJY22043-E error message is set. If this method is executed while the JP1/IM3 - Manager service is stopped, the KAJY32000-E message is set. For details about the error messages set in all the other cases, see the table under *Status codes* in *5.6.1 Event search*.
2	errorMessageId	Returns the ID of the error message.

In methods of a product plug-in that calls this method, consider error messages and error processing based on the specifications of the plug-in, according to the value of the key errorMessageId.

Output the key errorMessage to the internal log of the product plug-in for use in troubleshooting it.

Exception

None

4.5.14 jp1SimtService.getLink

This method retrieves link information.

This method cannot be called from the __eventGet method provided by product plug-ins or from the method called by the __eventGet method.

The details of the jp1SimtService.getLink method are provided below.

Method name

```
Object jp1SimtService.getLink(String type, String sid, int fromLayerCount,
int toLayerCount, int countPerLayer, int linkCount, String lang, String
jp1User, String jp1Token)
```

Parameters

type

Of the types of link information supported by the system, specify the one corresponding to the link information you want to retrieve. If you specify null or an empty string, applicable link information is returned regardless of link information type.

type describes a grouping of relations that have the same meaning. On the **Related node** tab in the Integrated Operation Viewer window, you can filter relations to display only those belonging to a specific type.

For relations within a JP1/IM product or between a JP1/IM product and another product, the following types are used. In addition to these types, the use of user-specified types is also allowed.

- rootJobnetExecutionOrder: Relation of the execution order of root jobnets
- managerAgent: Relation between the manager and agent of a JP1 product
- rootJobnetAgent: Relation between a root jobnet and an AJS agent
- sameNode: Relation between nodes with the same name
- L2Connection: Relation between layer-2 connection lines managed by JP1/NNMi
- Infrastructure: Relation between infrastructure resources managed by JP1/OA
- monitoringConfiguration: Relation between a product and a monitoring target in a monitoring product configuration

sid

Specify the SID of the node to be processed. Information regarding the nodes preceding and succeeding the specified node is returned. If you specify null or an empty string, link information on all nodes is returned.

fromLayerCount

Specify the maximum number of preceding node layers to be retrieved in the range from 0 to 2147483647. If you specify null or an empty string for sid, the value specified for the fromLayerCount parameter is ignored.

toLayerCount

Specify the maximum number of succeeding node layers to be retrieved in the range from 0 to 2147483647. If you specify null or an empty string for sid, the value specified for the toLayerCount parameter is ignored.

countPerLayer

Specify the maximum number of nodes to be retrieved per node layer in the range from 1 to 2147483647. If you specify null or an empty string for sid, the value specified for this argument is ignored.

linkCount

Specify the maximum number of links to be retrieved in the range from 1 to 2147483647. If you specify null or an empty string for sid, the value specified for the linkCount parameter is ignored.

lang

Specify the language of the message. You can specify ja, ja-JP, or en. If you specify any other values, it is assumed that en is specified. For details, see *Language conventions of user-created plug-ins* in *4.4 Methods implemented in the plug-in*.

jp1User

By using a string of 1 to 31 bytes, specify the name of a JP1 user who has one of the following JP1 permission levels:

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

jp1Token

Specify a JP1 authentication token for the JP1 user specified for jp1User.

Return values

After successful retrieval of link information, an object storing link information is returned. The following table describes the keys and their values stored in the object:

No.	Key			Value
1	links			Returns an array of retrieved link information. For details about the array of link information, see *IM management node link definition file (imdd_nodeLink_def.conf)* in *Chapter 2. Definition Files*.
2	exceedCountDetected			Indicates whether it has been detected that the value specified for the parameter has exceeded the maximum limit.
3		countPerLayer		Indicates whether it has been detected that the maximum number of nodes per layer has been exceeded.
4			layer*integer*	Replaces *integer* with the number assigned to each layer. 0 is assigned to the layer specified for sid, with the number assigned to the layers succeeding it incremented starting from +1, and that assigned to the layers preceding it decremented starting from -1. In this way, this key indicates for all layers returned whether it has been detected that the maximum number of nodes allowed per layer has been exceeded. • true Detected • false Not detected
5		linkCount		Indicates whether it has been detected that the maximum number of links allowed has been exceeded. • true Detected • false Not detected
6	messageId			A message ID. When there is no message to be provided, null is specified.
7	message			The body of a message. When there is no message to be provided, null is specified.

The following table describes the keys and their values stored in the object after a failed attempt to retrieve link information:

No.	Key	Value
1	`errorMessage`	An error message. When any of the arguments is invalid, the `KAJY22043-E` error message is output. For details about the error messages output in all the other cases, see the table under *Status codes* in *5.6.1 Event search*.
2	`errorMessageId`	Returns the ID of the error message.

In methods of a product plug-in that calls this method, consider error messages and error processing based on the specifications of the plug-in, according to the value of the key `errorMessageId`.

Output the key `errorMessage` to the internal log of the product plug-in for use in troubleshooting it.

Exception

None

4.5.15 jp1EmService.changeEventStatus

This method changes the event status. When the specified JP1 user does not have the permission to view the specified events, an error occurs. When the specified user does not have the permission to operate the specified events, the user is not allowed to operate the events. For details about the conditions under which a JP1 user may be able to view JP1 events, see information regarding the events a JP1 user can display in the event view after selecting an IM management node in *3.5.1 Structure of the IM management node* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

This method cannot be called from the `__eventGet` method provided by product plug-ins or from the method called by the `__eventGet` method.

The details of the `jp1EmService.changeEventStatus` method are provided below.

Method name

```
Object jp1EmService.changeEventStatus(int dealt, String[] sid, String lang,
String jp1User, String jp1Token)
```

Parameters

`dealt`

Specify one of the following values to indicate the event status after the change:

- `0` (Unprocessed)
- `1` (Processed)
- `2` (Processing)
- `3` (Held)

`sid`

Specify an array of SIDs corresponding to the JP1 events whose status you want to retrieve. For details about the SIDs of JP1 events, see *7.2.1 (1) Event information object*. You can specify a maximum of 2,000 SIDs of JP1 events.

lang

Specify the language of the message. You can specify ja, ja-JP, or en. If you specify any other values, it is assumed that en is specified. For details, see *Language conventions of user-created plug-ins* in *4.4 Methods implemented in the plug-in*.

jp1User

By using a string of 1 to 31 bytes, specify the name of a JP1 user who has one of the following JP1 permission levels:

- JP1_Console_Admin
- JP1_Console_Operator

jp1Token

Specify a JP1 authentication token for the JP1 user specified for jp1User.

Return values

After changes are made successfully to the event status, an object storing event information is returned. The following table describes the keys and their values stored in the object:

No.	Key	Value
1	eventData	Returns an array of event information objects representing a list of events whose statuses have been changed. For details about the event information objects, see *7.2.1 (1) Event information object*. When there are any events that the specified user did not have the sufficient permission to operate, only those events that the user succeeded in operating are returned.
2	messageId	Returns the message ID of a temporary error message generated during an event search. When there is no message to be provided, null is specified.

The following table describes the keys and their values stored in the object after a failed attempt to change the event status:

No.	Key	Value
1	errorMessage	An error message. When any of the arguments is invalid, the KAJY22043-E error message is set. If this method is executed while the JP1/IM3 - Manager service is stopped, the KAJY32100-E message is set. For details about the error messages set in all the other cases, see the table under *Status codes* in *5.6.1 Event search*.
2	errorMessageId	Returns the ID of the error message.

In methods of a product plug-in that calls this method, consider error messages and error processing based on the specifications of the plug-in, according to the value of the key errorMessageId.

Output the key errorMessage to the internal log of the product plug-in for use in troubleshooting it.

Exception

None

4.5.16 jp1SimtService.getTreeSid

This method retrieves the tree SID corresponding to the specified configuration information SID.

This method cannot be called from the __eventGet method provided by product plug-ins or from the method called by the __eventGet method.

The details of the jp1SimtService.getTreeSid method are provided below.

Method name

`String jp1SimtService.getTreeSid(String sid)`

Parameters

`sid`

Specify the configuration information SID.

Return values

A tree SID is returned.

When `null` is specified for `sid` or when there is no tree SID corresponding to the specified configuration information SID, `null` is returned.

Exception

None

4.5.17 jp1TrendDataService.getTrendData

This method retrieves trend data (time series data) from the trend data management DB.

Here are the details of the jp1TrendDataService.getTrendData method:

Method name

```
Object jp1TrendDataService.getTrendData(String jp1user, String sid, String
promQLQuery, String starttime, String endtime, String step)
```

Parameters

`jp1user`

Specify the JP1 user name in the range of 1~31 bytes.

If the SID specified by the sid argument specifies a SID for which the JP1 user specified by the jp1user argument does not have reference authority*, 0 data records are returned.

Note: This applies when a JP1 resource group with one of the following JP1 authorization levels is not set to the SID specified in the argument sid among the JP1 resource groups set for the JP1 user.

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

`sid`

Specifies the SID for the configuration information.

If the replacement string "`$jp1im_TrendData_labels`" is included in PromQL expression specified by the argument `promQLQuery`, it is replaced by value of the `jp1im_TrendData_labels` that is set in SID of the configuration information specified by the argument `sid` and passed to the trend data management service.

`promQLQuery`

Specify the filter conditions for trend data with PromQL statements.

For details about PromQL expression that can be specified, see *2.7.4(4) About PromQL* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`starttime`

Specifies the start time for fetching trend data in seconds elapsed since January 1, 1970 00:00:00 (UNIX epoch). You cannot specify a time (negative value) before 0:00:00 a.m. on January 1, 1970.

endtime

Specifies the end time for obtaining trend data in seconds elapsed since January 1, 1970 00:00:00 (UNIX epoch). You cannot specify a time (negative value) before 0:00:00 a.m. on January 1, 1970.

step

Specify the interval between getting trend data in seconds.

Return values

If the trend data acquisition is successful, the trend data object containing the trend data information is returned. For details on the format of trend data objects, see *7.2.3(1) Trend Data Object*.

If trend data fails to be retrieved, the keys and values stored in the object are shown below.

Key	Value
`errorMessage`	Error message. • If the jp1user argument is invalid, the message KAJY22043-E is set. • If the sid argument is invalid, a KAJY62003-E error message is set. • If the port number of the Trend Data Management Service fails to be obtained, the message KAJY62004-E is set. • If communication with the Trend Data Management Service fails, the message KAJY62000-E is set. • If the Trend Data Management Service returns an error, the message KAJY62002-E is set. • If the SID of the configuration information managed by the subordinate manager is specified and the connection to the intelligent integrated management infrastructure of the subordinate manager fails, the message `KAJY00027-E` is set. • If the SID of the configuration information managed by the subordinate manager is specified and an error occurs in the processing of the intelligent integrated management infrastructure of the subordinate manager, the message `KAJY00029-E` is set.
`errorMessageId`	Returns the ID of the error message.

The method of the user-created plug-in that calls this method determines the error by the presence or absence of the value of the key `errorMessageId`, and depending on the contents of the value, consider error messages and error handling based on the plug-in specifications.

Output the value of the key `errorMessage` to the internal log of the plug-in and use it for plug-in failure investigation.

Exception

None

4.5.18 jp1TrendDataService.getLabelList

This method retrieves a list of time series of label set Match to the parameter-specified criteria from Trend data Management Database of the respective manager.

Method name

```
Object jp1TrendDataService.getLabelList(String host, String[] match, String
starttime, String endtime, String jp1User)
```

Parameters

host

Specify host name of JP1/IM - Manager, from 1 to 255.

match

Specify the filter criteria for the label set to retrieve from Trend data Management Database.

More than one condition can be specified as an array. If specified, an OR condition is set. You can specify up to three conditions.

The criteria can be a metric. You can also add a comma-separated list enclosed in {} to specify a condition that compares a label with a label value enclosed in '. The following shows the operators and specification examples of comparison conditions.

- =: Match the specified text
- !=: Does not match the specified text.
- =~: Regex match to the specified string
- !~: Regex does not match on the specified string

(Example of specification)

- When creating IM management node for various Exporter
  When you retrieve a `up` metric label-set, you specify `up`.
- To create IM management node for Yet another cloudwatch exporter
  When retrieving a label set that starts with `aws_` in the `__name__` label, specify `{__name__=~'aws_.*'}`.
- To create IM management node for Fluentd
  When retrieving the `fluentd_logtrap_running` label set, specify the `fluentd_logtrap_running`.

`starttime`

Specifies the starting time for retrieving the list of label sets, in seconds since UTC 1970 January 1 00:00:00 (UNIX epoch). The time before midnight 0:0:0 on January 1, 1970 (minus Value) cannot be specified.

`endtime`

Specifies the ending time for retrieving the list of label sets, in seconds since UTC 1970 January 1 00:00:00 (UNIX epoch). The time before midnight 0:0:0 on January 1, 1970 (minus Value) cannot be specified.

`jp1User`

Specify JP1 user name with the following JP1 Permissions level in the range of 1~31 bytes.

- JP1_Console_Admin

Return values

If the list of label sets is successfully retrieved, the list of label sets is returned. For the format of the list of label sets, see *7.2.3(2) Label Set List Object*.

The following table lists the keys and value that are stored in the object when retrieving the list of label sets fails.

Key	Value
`errorMessage`	Error message. • If the Trend Data Management Service fails to retrieve Port number, KAJY62004-E's message is Setup. • If communication with the Trend Data Management Service fails, KAJY62000-E's message is Setup. • If the Trend Data Management Service returns Error, KAJY62005-E's message is Setup. • If the specified host fails to connect to Intelligent Integrated Management Base, KAJY00027-E's message is Setup. • If Intelligent Integrated Management Base operation on the specified host fails, KAJY00029-E's message is Setup.
`errorMessageId`	Returns id of the error message.

For user-created plug-in method that invokes this method, determine error with or without value of `errorMessageId` key. Depending on the content of value, consider error messages or error handling based on the plug-in specification.

The key `errorMessage` value is output to the plug-in's internal log. It can be used to investigate plug-in failures.

Exception

None

4.6 File name and the storage location of the user-created plug-in

You can specify any given name for the file name of the user-created plug-in. The name must follow the rules below.

- Characters available for the file name: Alphanumeric characters
- Extension: `.js` at all times
- The following file names are not available. The file name is case insensitive.
  File name that starts with `jp1` or `hitachi`

The user-created plug-in should be located in the directory with the same name as the file name of the plug-in. In a single directory, you can put only one file with the same name as the directory.

The following shows an example of creating the user-created plug-in named `userPlugin.js`.

In Windows:

On a physical host:

Manager-path`\plugin\imdd\userPlugin\`

On a logical host:

shared-folder`\jp1imm\plugin\imdd\userPlugin\`

In UNIX:

On a physical host:

`/etc/opt/jp1imm/plugin/imdd/userPlugin/`

On a logical host:

shared-directory`/jp1imm/plugin/imdd/userPlugin/`

If you create a directory named `user` as a storage location for a plug-in, the `user` directory can contain some user-created plug-ins with a given file name.

4.6.1 Definition files used by user-created plug-ins

The following shows where the definition files used by user-created plug-ins are located.

In Windows:

On a physical host:

Manager-path`\conf\imdd\plugin\`*product-name*#`\`

On a logical host:

shared-folder`\jp1imm\conf\imdd\plugin\`*product-name*#`\`

In UNIX:

On a physical host:

`/etc/opt/jp1imm/conf//imdd/plugin/`*product-name*#`/`

On a logical host:

shared-directory`/jp1imm/conf/imdd/plugin/`*product-name*#`/`

#: *product-name* can be:

- In JP1/AJS: jp1ajs
- In JP1/PFM: jp1pfm

File

- *file-name*`.`*extension*
- *file-name*`.`*extension*`.model`

Include *file-name*`.`*extension*`.model` and create a file with the name of *file-name*`.`*extension* during installation. During upgrade installation, only *file-name*`.`*extension*`.model` is overwritten.

4.7 Applying changes made to user-created plug-ins

When you make changes to user-created plug-ins, you have to restart the JP1/IM3 - Manager service.

5 API

This chapter describes the APIs provided by JP1/IM - Manager (Intelligent Integrated Management Base).

5.1 List of APIs

The following table lists APIs that can be used with the user-created plug-in of JP1/IM.

Table 5–1: List of APIs of the user-created plug-in (API related to JP1/IM - Manager)

Category	API name	Description
User authentication	Login	Logs in to the Intelligent Integrated Management Base.
	Logout	Logs out from the Intelligent Integrated Management Base.
	Initial secret issue	Issue initial secret.
	IM Client secret delete	Delete IM client secret that you have added to the database.
	IM Client secret issue	Issue IM client secret and add it in the database.
	IM Client list acquisition	Retrieve a list of added IM client IDs.
Link information	Link information acquisition	Gets the link information that represents order relationships between objects.
	Link type list acquisition	Gets the list of types of link information.
Event management	Event search	Searches the integrated monitoring database for events based on specified conditions.
	Event detailed information acquisition	Gets the details of a specified event.
	Event status change	Changes the event status of specified events.
	Event generation	Generates the specified event.
	JP1 Event converter	This function converts event data reported from an external system to JP1 events and issues them.
Performance information	Plug-in processing execution	Executes plug-in operations for performance information.
System status monitoring	IM management node related information generation	Obtains the system configuration information and generates a configuration management tree File.
	IM management node related information reflection	Reflect configuration management tree file in Intelligent Integrated Management Base.
	IM management node information acquisition	Gets the information of IM management nodes collected from JP1/AJS3, JP1/PFM, JP1/IM, JP1/Base, and others.
	Configuration management tree information acquisition	Gets the configuration information of IM management nodes (management groups or management objects) as a tree.
	IM management node status acquisition	Gets the status information of all IM management nodes (management groups or management objects).
	Suggestion mapping information acquisition	Gets information regarding the mapping between IM management nodes and suggestion IDs.
Proxy	Proxy credential setup	Sets the authentication user and password of the proxy server.
Linked product	URL information acquisition	Gets the URL to start a linked product configured in an IM management node.
Trend	Metric list acquisition	Gets the list of metrics for the specified SID.
	Time-series data acquisition	Gets time-series data for the specified SID.
	Write Trend Data	Writes trend data to Trend data Management Database. The data to be written can be specified in JSON format.

Category	API name	Description
Information management	Version information acquisition	Gets the JP1/IM version and REST API versions.
Suggestion	Previous execution history acquisition	Gets a history of previously executed response actions.
	Response action suggestion	Suggests response actions appropriate to the system status.
	Response action execution	Executes a response action.
OpenID authentication	Single sign-on mapping definition application	Applies the mapping information defined in the single sign-on mapping definition file (`imdd_sso_mapping.properties`) to the Intelligent Integrated Management Base.
Distribution	Get distribution (File download)	Downloads the distribution specified in the request line (File).
Execute for Auto/ Manual Response Action	Obtain execution result of Response Action	Get Execute of Response Action.
	Manual execution of Response Action	Response Action(manual) is performed.
	Convert event-takeover info	Event information is inherited.
Definition file Manipulation	Get definition file list	Retrieves a list of definition file.
	Get definition file	Retrieve the definition file.
	Delete definition file	Delete the definition file.
	Updated definition file	Update definition file.
Integrated agent Administration	Retrieve integrated agent info	Retrieve integrated agent info.
	Delete integrated agent info	Delete integrated agent info.
	Retrieve Secret List	Retrieve a list of secrets that JP1/IM agent control base manages.
	Add, update, delete the secrets	Add, update, and delete the secrets that you want JP1/IM agent control base to manage.
Lower manager Info Management	Retrieve lower manager info list	Retrieve the base and relay manager under the control of Integrated manager.
	Add lower manager info	Add the base or relay manager under the information of Integrated manager.
	Delete lower manager info	Delete the base or relay manager under the control of Integrated manager.

Table 5–2: List of APIs of the user-created plug-in (API related to JP1/IM - Agent)

Category	API name#	Description
Prometheus server	Reload Prometheus server	Refreshes Prometheus server definition file and reflects it in Prometheus server operation.
	Prometheus server health check	Performs a health check of Prometheus server. The status code always returns 200.
Alertmanager	Reload Alertmanager	Refreshes Alertmanager definition file and reflects it in Alertmanager operation.
	Alertmanager health check	Performs a health check of Alertmanager. The status code always returns 200.
	Get silence list of Alertmanager	Retrieves a list of silence created in Alertmanager in JSON format.

Category	API name#	Description
	Silence creation of Alertmanager	Pass JSON form of silence's setting and create a silence in Alertmanager.
	Silence Revocation of Alertmanager	Revokes (expires immediately) silence created in Alertmanager.
	Get silence of Alertmanager	Retrieves the specified silence in JSON format.
Blackbox exporter	Reload Blackbox exporter	Refreshes Blackbox exporter definition file and reflects it in Blackbox exporter operation.
API for scrape of Exporter used by JP1/IM - Agent		Execute scrape of Exporter for which you want to scrape Prometheus server.

#

API do not have access-control functions. You can limit the source hosts of API by specifying a connectable IP address for the ports that the firewall allows.

5.2 API common specifications

Monitored information collected by JP1/IM - Manager (Intelligent Integrated Management Base) can be accessed by using API via http(s).

The API provided with the Intelligent Integrated Management Base is based on the REST (Representational State Transfer) architecture style.

5.2.1 Communication methods

The API uses the communication protocols and the port number described below. For API communication, you can use the http or https protocol.

Communication protocols

HTTP, HTTPS

Port number

20703

For details on the port number, see *Intelligent Integrated Management Base definition file (imdd.properties)*in *2. Definition Files*.

5.2.2 Input/Output format

The JSON format is used for the data of API requests and responses. The data is encoded in UTF-8.

5.2.3 Request format

To access the functionality provided by the Intelligent Integrated Management Base through the API, compose a request as follows:

```
method /application/component/apiVersion/resourceId?query httpVersion
requestHeader

messageBody
```

The following table describes how to compose a request.

Table 5–3: Request format in detail

Item	Description
method	Specify how to operate the resource. Select a method appropriate to the API processing. The API supports the following methods: • `GET` Gets a list of resources or their information. • `POST` Enables the Intelligent Integrated Management Base to process the resource. • `PUT`

Item	Description
	Updates a list of resources or their information. - DELETE Deletes a list of resources or their information. For details on the method you specify, see *Format* for each API.
application	The name of the application that provides the API. Always set this to `im`.
component	The component name of the API. Specify `api` for APIs used by the user, and `api_system` for APIs used by the system. Note that the APIs that can be used for *5.2.8(4) Authentication through client secret information added to a REST API (Basic authentication)* are limited to APIs with component name `api_system`.
apiVersion	The API version. Always set this to `v1`.
resourceId	The functions provided by the Intelligent Integrated Management Base can be identified by specifying a resource identifier in an API request. Specify the identifier of a function that you want to run. For details, see *Table 5-4 Resource identifiers*.
query	The query string. You can add search conditions to a request to filter or sort records to be returned in a response.
httpVersion	The version of the communication protocol that the API uses. Always set this to `HTTP/1.1`.
requestHeader	Specify the data format, language code, and other settings of the response. For details, see *Table 5-5 Request headers*.
messageBody	Specify the data format of the message body. You can use the JSON format. The data is encoded in UTF-8.

Table 5–4: Resource identifiers

Resource identifier	Resource to be accessed
`nodes`	Management nodes
`status`	Status information
`links`	Link information (relationship of jobnets or others)
`events`	JP1 events
`actions`	Plug-in actions (getting performance information or others)
`login`	Login token or permissions
`proxyUsers`	Proxy user information

Table 5–5: Request headers

Header	Description	Default value	Required/ Optional
`Authorization`	Specify the authentication information for the API. This must be specified if permission is required for the user to invoke the API. For details on the authentication information and how to set the authentication information to invoke the REST API, see *Authentication methods for REST API*.	None	Required
`Accept-Language`	Specify the language you want to use in response data with one of the following language codes: - `ja` or `ja-JP` Japanese	`en`	Optional

Header	Description	Default value	Required/ Optional
	- en English Omitting this header or specifying any value other than acceptable values causes en to be used. The status code 200 is returned regardless of the specified value.		
Content-Type	The data format of the request message body. Omitting this header when using the POST method or specifying an invalid value results in the status code 415 to be returned. If you use the POST method and there is no message body, or if you use the GET method and you specify a value other than application/json, the status code 200 is returned.	None	Required
Content-Length	Specify the length of the message body in the request. - For the GET method: Omit this header or specify 0. - For the POST method: Specify the size (in bytes) of the request body. This must be specified as a decimal number. Omitting this header when using the POST method is results in the status code 411 to be returned. If you use the POST method and you have specified the request body of which the size exceeds the specified size, the status code 500 is returned. If you use the POST method and there is no message body, or if you use the GET method, the status code 200 is returned.	None	- Optional GET method - Required POST method
Accept	The data format of the response message body. Always set this to application/json. if you use the POSTmethod and you specify a value other than application/json, the status code 406 is returned. If you use the POST method and there is no message body, or if you use the GET method and you specify a value other than application/json, the status code 200 is returned.	application/json	Optional
Cookie	If you issue REST API requests consecutively without logging in again, specify cookie information for login API responses. Specifying cookie enables the session to be maintained, eliminating the need to log in or out every time you issue a REST API request. The session is discarded automatically three minutes after the last REST API request is issued. If you do not want to maintain the session, you do not have to specify this header. In addition, do not specify it if you use authentication (Basic authentication) with login information added to a REST API.	None	Optional

If you specify a property that is not listed in the table above, the property is ignored.

5.2.4 Limitation on the request body size

JP1/IM API limits the request body size to less than 10 MB. If the size exceeds 10 MB, the status code 413 is returned and the error message KAJY00009-E is issued. For details on the message, see the *JP1/Integrated Management 3 - Manager Messages*.

5.2.5 Response format

The following describes the format of a response:

```
httpVersion statusCode
responseHeader

messageBody
```

Table 5–6: Response format in detail

Item	Description
httpVersion	As the version of the communication protocol used by an API, `HTTP/1.1` is returned.
statusCode	Returns a status code that indicates the result of the processed request.
responseHeader	Returns the data format of the response, which was specified in the request header.
messageBody	Returns the message body data as follows: • Data format: JSON • Encoding: UTF-8

(1) Status codes

The following table lists status codes to be returned when an API is run. Possible returned status codes are different for each API. For details, see the description of each API.

Table 5–7: Status codes

Status code	Message	Description
`200`	For details, see the description of each API.	The request was processed successfully.
`400`	`Bad-request`	The request is invalid.
`401`	`Unauthorized`	Could not be authenticated. Information for authentication or authorization is invalid.
`403`	`Forbidden`	There is no permission to run the request.
`404`	`Not-found`	The requested resource is not found or no operation is found for the resource. Or a specified parameter is invalid.
`406`	`Not-acceptable`	The specified response format is not supported.
`411`	`Length Required`	When the `POST` method is used, the `Content-Length` property of the request header is omitted.
`413`	`Payload Too Large`	The size of the request body exceeds the upper limit.
`415`	`Unsupported media type`	The specified request format is not supported.
`500`	`Server-error`	An error occurred with the server processing.
`503`	`Service Unavailable`	The Intelligent Integrated Management Base service is unavailable. This might be caused by a temporal congestion or other reason.

(2) Response header

The following table describes response headers controlled by the Intelligent Integrated Management Base.

Table 5–8: Response header

Header	Description
Cache-Control	Specify the following so that the API response is not cached. --- Cache-Control: no-store, no-cache, max-age=0 Pragma: no-cache Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type	The data format of the response data. application/json is always returned as a fixed value.
WWW-Authenticate	Indicates that authentication is required when authentication with login information added to a REST API (Basic authentication) is used. --- WWW-Authenticate: Basic realm="JP1 Authentication Realm"

5.2.6 Error response message

The following exception object is returned in the response message body if the status code is not 200:

```
{
"timestamp":1539923958358,
"status":403,
"error":"Forbidden",
"exception":"jp.co.hitachi_solutions.it_service_cooperation_framework.securi
ty.ImDdBadCredentialsException",
"message":"Login processing failed due to an invalid parameter.,
"path":"/im/api/v1/login",
"messageId":"KAJY52001-E",
"returnCode":3
}
```

Table 5–9: Error response format in detail

Item	Description
timestamp	Specifies the elapsed time (in milliseconds) since 1970-01-01 00:00 in UTC.
status	statusCode in response format
exception	The class of the exception object
message	The message stored in the exception object. (A string obtained by Throwable#getMessage())
path	The path and subsequent string in the URI of the issued REST API
messageId	The JP1 message ID
returnCode	The return value of the REST API
extensions	Extended response information

5.2.7 Data types

The following table describes data types supported by JP1/IM API.

Table 5–10: Supported data types

Data type	Description
boolean	`true` or `false`
int	32-bit signed integer
long	64-bit signed integer
string	Text data Unless otherwise specified, a number is handled as a decimal number if dealt with as string type.

If you use a character listed in the following table as string type in JSON format, use the escape character for it.

Table 5–11: String type characters that need to be escaped in JSON format

Character	Escaped character
Double quotation mark (")	`\"`
Backslash (\\)	`\\`
Backspace	`\b`
Form feed	`\f`
Line feed	`\n`
Carriage return	`\r`
Tab	`\t`

Dates and times must be specified in the ISO8601 format, as described below. Return values also take the same format.

Format

```
YYYY-MM-DDThh:mm:ssTZD
```

Table 5–12: Format of the date and time

Placeholder	Description	Acceptable value
YYYY	Specifies the year.	`1994` to `2099` (year)
MM	Specifies the month.	`01` to `12` (month of the year)
DD	Specifies the day.	`01` to the last day of the specified month (day of the month)
hh	Specifies the hour.	`00` to `23` (hour)
mm	Specifies the minute.	`00` to `59` (minute)
ss	Specifies the second.	`00` to `59` (second)
TZD	Specifies the time difference between the time zone of the specified value and Coordinated Universal Time (UTC).	• For UTC `Z` • For time zones other than UTC `+`*hh*`:`*mm* or `-`*hh*`:`*mm*

For example, 2019-03-01 12:00:00 in UTC is represented by `2019-03-01T21:00:00+09:00` in Japan Standard Time, or `2019-03-01T07:00:00-05:00` in US Eastern Standard Time.

In some countries and territories, the daylight saving time must be considered. For example, IM-DD specifies `2019-04-01T08:00:00-04:00` in US Eastern Standard Time (Daylight Saving Time) to represent 2019-04-01 12:00:00 in UTC.

5.2.8 Authentication methods for REST API

In order for users to issue API requests and get responses, they must be authenticated first. The following types of authentication are available on the Intelligent Integrated Management Base:

- Authentication by using the login API
- Authentication through login information added to a REST API (Basic authentication)
- Authentication through login information added to a REST API (OpenID authentication)
- Authentication through client secret information added to a REST API (Basic authentication)

(1) Authentication by using the login API

The following describes steps for authentication with the login API.

1. Invoke the login API.

   Provide the JP1 user name and password to be authenticated and then, if successful, receive the token string and cookie string. For details on the login API, see *5.4.1 Login*.

2. Invoke a REST API.

   To invoke a REST API, set the following HTTP request header with the token string that was retrieved by the login API.

   You can invoke the REST APIs other than login and logout.

   Request header

   `Authorization`

   Value to be specified

   `Bearer` *token-string*

   Example of a specification

   For example, if the token string `anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2p` is obtained by the login API, specify as follows:

   ```
   Authorization: Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2p
   ```

3. Invoke the logout API.

   Use the cookie string that was retrieved by the login API to discard the authentication information that is used for the current login. For details on the logout API, see *5.4.2 Logout*.

(2) Authentication through login information added to a REST API (Basic authentication)

The following shows the procedure for Basic authentication through login information added to a REST API.

By default, the Basic authentication setting is disabled. To enable it, set the `jp1.imdd.authBasic` property to `true` in the Intelligent Integrated Management Base definition file (`imdd.properties`).

For details on the Intelligent Integrated Management Base definition file (`imdd.properties`), see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files*.

1. Invoke a given REST API.

   In the HTTP request header on invocation of a REST API, specify `Basic` as the authentication method, followed by a Base64-encoded string of the user name concatenated with the password using `:` (ASCII: 0x3A) (which is called a *basic token*).

   Request header

   `Authorization`

   Value to be specified

   `"Basic "` + Base64-encoded ASCII string of JP1-*user-name*`:`*password*

   Example of a specification

   If the JP1 user is `jp1user` and the password is `password`, then use the Base64-encoded string of `jp1user:password`, `anAxdXNlcjpwYXNzd29yZA==`, to specify the basic token as shown below:

   ```
   Authorization: Basic anAxdXNlcjpwYXNzd29yZA==
   ```

Important

- Do not specify any cookie in the request header because Basic authentication is a stateless authentication method.
- Basic authentication can be used with either of HTTP or HTTPS, but we recommend access over HTTPS for better security.
- The authentication server performs authentication every time a REST API is executed, and therefore each authentication operation outputs a message related to the user management function to the server. If the authentication server also has a system that outputs integrated trace logs, design the system configuration with the possibility that the messages related to the user management function may cause a high load on the integrated trace in mind.

(3) Authentication through login information added to a REST API (OpenID authentication)

The following shows a procedure for OpenID authentication by using login information added to a REST API.

OpenID authentication is disabled by default. To enable it, you have to edit the OpenID provider-related properties provided in the Intelligent Integrated Management Base definition file (`imdd.properties`).

For details on the Intelligent Integrated Management Base definition file (`imdd.properties`), see *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files*.

1. Invoke a REST API.

   In the HTTP request header for invoking a REST API, specify `Bearer` as the authentication method, and then the access token submitted by the OpenID provider.

   Request header

   `Authorization`

Value to be specified

`Bearer` *string-representing-access-token*

- When multiple OpenID providers are set as the authentication infrastructures on the Intelligent Integrated Management Base, you must specify the key name (access token issuer) of the OpenID provider in the HTTP request header `X-Token-Issuer` that is used to invoke a REST API. The key name that you specify here must be the one that is defined in the Intelligent Integrated Management Base definition file (`imdd.properties`).
- If, upon the acceptance of the processing of the REST API by the Intelligent Integrated Management Base, it turns out that the HTTP request header `X-Token-Issuer` is not specified or that the value specified for `X-Token-Issuer` does not match the OpenID provider's key name defined in the Intelligent Integrated Management Base definition file (`imdd.properties`), an authentication error occurs. In this case, the status code `403` and the error message `KAJY52030-E` are returned to the caller of the REST API.
- When only one OpenID provider is set as the authentication infrastructure on the Intelligent Integrated Management Base, you do not have to specify the HTTP request header `X-Token-Issuer` that is used to invoke a REST API. When this HTTP request header is not specified, the Intelligent Integrated Management Base processes the REST API assuming that the OpenID provider defined in the Intelligent Integrated Management Base definition file (`imdd.properties`) is the access token issuer.
- `X-Token-Issuer` is a unique request header defined in the Intelligent Integrated Management Base, which has the following format:

Request header	Value to be specified
`X-Token-Issuer`	Name of the OpenID provider that issued the access token. Specify the value representing the OpenID provider's key name defined in the Intelligent Integrated Management Base definition file (`imdd.properties`).

Example 1

- The access token is issued by Keycloak.

- Only one OpenID provider is set as the authentication infrastructure on the Intelligent Integrated Management Base definition file.

The key name of the OpenID provider (Keycloak)

- The access token submitted by the OpenID provider is `ABCDEFG.HIJKLMN.OPQRSTUVWXYZ`.

Under the conditions described above, set the access token in the request header as follows:

```
Authorization: Bearer ABCDEFG.HIJKLMN.OPQRSTUVWXYZ
```

Example 2

- The access token is issued by Keycloak.

- Multiple OpenID providers (Keycloak and Okta) are set as the authentication infrastructures on the Intelligent Integrated Management Base.

The key name of one OpenID provider (Keycloak)

The key name of the other OpenID provider (Okta)

- The access token submitted by the OpenID provider is `ABCDEFG.HIJKLMN.OPQRSTUVWXYZ`.

Under the conditions described above, set the access token and the token issuer in the request headers as follows:

```
Authorization: Bearer ABCDEFG.HIJKLMN.OPQRSTUVWXYZ
X-Token-Issuer: Keycloak
```

Important

- Although HTTP and HTTPS are both supported, we strongly recommend the use of HTTPS for OpenID authentication to protect against man-in-the-middle attacks. During operation, make sure to use HTTPS for access.
- In order to allow the JP1 user name used with the Intelligent Integrated Management Base to be mapped with the user name registered with the OpenID provider, the `preferred_username` claim of the access token must contain the name of the user logging in to the Open ID provider. When Keycloak is the issuer of the access token, the `preferred_username` claim is set in the access token by default. When Okta is the issuer of the access token, you must manually set the `preferred_username` claim. For details on how to set the `preferred_username` claim, see the document supplied by Okta.

  When the `preferred_username` claim is not set, the error message `KAJY52028-E` is returned. For details on the single sign-on mapping definition, see *Single sign-on mapping definition file (imdd_sso_mapping.properties)* in *Chapter 2. Definition Files*.

(4) Authentication through client secret information added to a REST API (Basic authentication)

The following shows the flow of Basic authentication based on client secret data added to REST API. This authentication is also used for integrated agent to Integrated manager communication and is therefore enable at all times. In addition, REST API on which this authentication can be used is limited to API used by the system. For details, see *3.7 Initial secret and client secret* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Because this authentication does not use JP1 users, it does not handle Login and Log out. In addition, the privilege does not set the privilege to the client (subject to authentication), so access-restriction by the privilege is not performed.

The outcome of authentication is printed to the secret authentication logging file.

1. Call any REST API.

   In HTTP request header at the time of REST API call, specify authentication method (you can specify `Basic` or `basic_auth`) followed by Base64 encoded string-called client token-that is the concatenation of user name and password with "`:`" (ASCII:0x3A).

   Request header

   `Authorization`

   Value to be specified

   - In case of specifying `Basic` as the authentication method:

   "`Basic  `" + Base64-encoded ASCII string of *client-ID*`:`*client-secret*

   - In case of specifying `basic_auth` as the authentication method:

   "`basic_auth  `" + Base64-encoded ASCII string of *client-ID*`:`*client-secret*

   Example of a specification

   If the client ID is `>client` and the client secret is `secret`, then use the Base64-encoded string of `>client:secret`, PmNsaWVudDpzZWNyZXQ=, to specify the basic token as shown below:

   - In case of specifying `Basic` as the authentication method:

   ```
   Authorization: Basic PmNsaWVudDpzZWNyZXQ=
   ```

   - In case of specifying `basic_auth` as the authentication method:

   ```
   Authorization: basic_auth PmNsaWVudDpzZWNyZXQ=
   ```

Important

- Do not specify any cookie in the request header because Basic authentication is a stateless authentication method.
- Basic authentication can be used with either of HTTP or HTTPS, but we recommend access over HTTPS for better security.

5.3 Explanation format for an API

The following lists sections to explain an API. Some sections are applicable only for some APIs, but not for others.

Description

Describes what you can do with the API.

Execution permissions

Lists permissions and roles required to run the API.

API version

Indicates the API version.

Format

Describes API request and response formats.

Parameters

Describes parameters to be specified in the request message body.

Status codes

Describes status codes that are returned as a response to the API that is run over the http or https protocol. For details on the status codes when an error occurs before an API is run, see *5.2.5(1) Status codes*.

Return values

Describes return values that are returned by the API.

Examples

Describes request and response examples to use the API.

Note that examples in this chapter use the http protocol. If you want to use the https protocol, you need to replace `HTTP` with `HTTPS`.

5.4 API for user authentication

This section describes operations related to the API for user authentication.

5.4.1 Login

Description

Logs in to the Intelligent Integrated Management Base according to the specified request.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/login/ httpVersion
```

Request message body

```
{
    "user":user-name,
    "password":password
}
```

Response message body

```
{
    "jp1user":JP1-user,
    "jp1token":JP1-authentication-token,
    "token":Authorization-header-authentication-token,
    "clientId":client-ID,
    "permissions":[
        JP1-user-permissions, ...
    ]
}
```

Parameters

`user`

Specify the user name as a string value.

`password`

Specify the password as a string value.

Status codes

The following table describes the status codes that are returned as a response to the request.

Status code	Message	Description
200	--	The login succeeded.

Status code	Message	Description
403	KAJY52001-E	The login failed due to an invalid parameter.
	KAJY52002-E	Could not communicate with the server that stores authentication data.
	KAJY52003-E	The login failed due to an internal error.
	KAJY52004-E	There is no permission to log in.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response header:

Parameter name	Description
`Set-Cookie`	Cookie string

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`jp1user`	string	The JP1 user name
2	`jp1token`	string	The JP1 authentication token
3	`token`	string	The authentication token for the `Authorization` header
4	`clientId`	string	The identifier to identify the client uniquely
5	`permissions`	array	An array of JP1 permission strings

The following exception object is returned in the response message body if the status code is not `200`:

No.	Member name	Data type	Description
1	`returnCode`	string	Detailed reason code

Examples

Example of invoking the login API

```
POST http://hostname:xxxxx/im/api/v1/login HTTP/1.1

{
    "user": "jp1admin",
    "password":"password"
}
```

Example of a response to the login API

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONID=7F2FB43CF4829025661D9E139E911B3B

{
    "jp1user": "jp1admin",
    "jp1token": "MGFkMmM2M2UwMDE4XzI3XzA4OjI0OjMzX19fX19fX19fX19fX19fX2
pwMWFkbWluICAgICAgICAgICAgICAgICAgICAgICAg",
    "token": "anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJME9qTXpYM
TlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJQ0FnSUNB
Z0lDQWdJQ0Fn",
    "clientId": "02157e39-2248-4a0e-8b63-78ffb4296e28",
    "permissions": {
        "*": [/*omitted*/]
    }
}
```

5.4.2 Logout

Description

Discards the authentication information that is used for the current login.

Execution permissions

None.

API version

v1

Format

Request line

```
POST /application/component/apiVersion/logout/ httpVersion
```

Request header

```
Cookie:cookie-information
```

Request message body

None.

Response header

```
Set-Cookie:cookie-information
```

Response message body

```
true
```

Parameters

`Cookie`

Specify the cookie string.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	--	The logout succeeded.

Return values

The following information is returned in the response header:

Parameter name	Description
`Set-Cookie`	Cookie string

Examples

Example of invoking the logout API

```
POST http://hostname:xxxxx/im/api/v1/logout HTTP/1.1
Cookie: JSESSIONID=7F2FB43CF4829025661D9E139E911B3B
```

5.4.3 Initial secret issue

Description

Issue initial secret.

To work with the manager, you must allocate client secret for each client that you want to authentication. Working with managers until they get client secret is one that is assigned to the manager and can temporarily use initial secret that is shared by all requestors.

The secret you publish is stored in integrated agent host administration DB.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/secret/generateInfo httpVersion
```

Request message body

None

Response message body

```
{
  "secret": secret-for-authentication,
  "lastUpdateTime": generation-date/time-of-secret
}
```

Parameter

None

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
403	KAJY01000-E	Insufficient privilege for the user used for authentication.
500	KAJY68001-E	DB accessible error

Return values

The following information is returned in the response body if the status code is 200:

Member name	Data type	Description
`secret`	`string`	Issued secret
`lastUpdateTime`	`string`	Secret publishing date/time The format is UTC time of day "*YYYY-MM-DD*T*hh*:*mm*:*ss*Z" in ISO8601 extended format.

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Examples

The example below executes the API:

Request:

```
POST http://immhost01:20703/im/api/v1/secret/generateInfo
```

Manager host name: `immhost01`

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json

{
    "secret": "Issued-secret",
    "lastUpdateTime": "2022-10-20T12:25:45Z"
}
```

5.4.4 IM Client secret delete

Description

Delete IM client secret that was added to the database.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/secret/client/deleteInfo httpVer
sion
```

Request message body

```
{
    "clientIds": [ IM-client-ID, .... ]
}
```

Here are the parameters that you specify for message body of the request:

Member name	Data type	Optional	Description
`clientIds`	`string[]`	No	Specifies the listing of ID of IM client secret that you want to delete. When working with JP1/IM, the elements of a listing can be any text. However, the following character strings cannot be specified: • String beginning with "`AGENT_`" • Strings beginning with "`MANAGER_`" other than "`MANAGER__INTEGRATED_host name`" The number of characters that can be specified is 1~280, and the characters that can be specified are ASCII codes (0x20~0x7e (excluding ":").

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	--	API operation was successful.
`400`	`KAJY68002-E`	The request parameter is invalid.
`403`	`KAJY01000-E`	Insufficient privilege for the user used for authentication.
`500`	`KAJY68007-E`	• DB accessible error • The specified IM client ID is not added on DB.

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Examples

The example below executes the API:

Request:

```
POST http://immhost01:20703/im/api/v1/secret/client/deleteInfo

{
    "clientIds": [ "clientId1", "clientId2" ]
}
```

Manager host name: `immhost01`

Response:

```
< HTTP/1.1 500 Internal Server Error
< Content-Type: application/json
{
    "timestamp": 1585561108345,
    "status": 500,
    "error": "Internal Server Error",
    "exception":"XXXXXXXXXXXXXXXXXXXXXXX",
    "message": "Failed to delete an IM client secret.",
    "path": "/im/api/v1/secret/client/deleteInfo ",
    "messageId": " KAJY68007-E"
}
```

5.4.5 IM Client secret issue

Description

Issue IM client secret.

When linking a manager host with a user-specific OSS, or a CloudWatch Logs/AzureMonitor provided by JP1/IM - Manager or lower manager, use IM client secret to perform authentication by communicating with the intelligent integrated management infrastructure and the partner.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/secret/client/generateInfo httpV
ersion
```

Request message body

```
{
    "clientId": IM-client-ID
}
```

Response message body

```
{
  "clientSecret": IM-client-secret-for-authentication,
  "lastUpdateTime": IM-client-secret-issue-date/time
}
```

Here are the parameters that you specify for message body of the request:

Member name	Data type	Optional	Description
clientId	string	No	Specifies the listing of ID of IM client secret that you want to issue. When working with JP1/IM, the elements of a listing can be any text. However, the following character strings cannot be specified: • String beginning with "AGENT_" • String beginning with "MANAGER_" The number of characters that can be specified is 1~280, and the characters that can be specified are ASCII codes (0x20~0x7e (excluding ":").

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68002-E	The request parameter is invalid.
400	KAJY68004-E	The same IM client ID has been added.

Status code	Message	Description
403	KAJY01000-E	Insufficient privilege for the user used for authentication.
500	KAJY68008-E	DB accessible error

Return values

The following information is returned in the response body if the status code is 200:

Member name	Data type	Description
clientSecret	string	Issued IM client secret
lastUpdateTime	string	IM client secret publishing date/time The format is UTC time of day "*YYYY*-*MM*-*DD*T*hh*:*mm*:*ss*Z" in ISO8601 extended format.

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Examples

The example below executes the API:

Request:

```
POST http://immhost01:20703/im/api/v1/secret/client/generateInfo
{
    "clientId": "clientSecret1"
}
```

Manager host name: immhost01

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
{
    "clientSecret": "Issued-IM-client-secret",
   "lastUpdateTime": "2022-10-20T12:25:45Z"
}
```

5.4.6 IM Client list acquisition

Description

Retrieves a list of IM client ID that have been added.

When linking the manager host with your own OSS, or CloudWatch Logs/AzureMonitor provided by JP1/IM - Manager or lower manager, use IM client secret to authentication communication between Intelligent Integrated Management Base and the partner.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
GET /application/component/apiVersion/secret/client/list httpVersion
```

Request message body

None

Response message body

```
{
  "clientIds": [IM-client-ID,...]
}
```

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	--	API operation was successful.
`403`	`KAJY01000-E`	Insufficient privilege for the user used for authentication.
`500`	`KAJY68009-E`	DB accessible error

Return values

The following information is returned in the response body if the status code is `200`:

Member name	Data type	Description
`clientIds`	`string[]`	Array of ID identifying IM client secret

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Examples

The example below executes the API:

Request:

```
GET http://immhost01:20703/im/api/v1/secret/client/list
```

Manager host name: `immhost01`

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
{
    "clientIds": [ "clientid1", "clientid2" ]
}
```

5.5 API for link information

This section describes operations related to API of link information.

5.5.1 Link information acquisition

Description

Gets the link information that represents order relationships between objects, such as jobs.

When link information is registered in the system, the link information that satisfies the specified criteria, such as before or after a particular object, is retrieved.

Execution permissions

See *Appendix E.1 Operating permissions required for system monitoring using the Intelligent Integrated Management Base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

API version

v1

Format

Request line

```
POST /application/component/apiVersion/links httpVersion
```

Request message body

```
{
"type": type-of-the-target,
"sid": target-IM-management-node-SID,
"fromLayerCount": layer-count-of-the-preceding-node,
"toLayerCount": layer-count-of-the-succeeding-node,
"countPerLayer": node-count-per-layer,
"linkCount": node-relationship-count
}
```

Response message body

```
{
    "links": [
        {
            "from": the-preceding-node-SID,
            "to": the-succeeding-node-SID,
            "type": type-of-the-target
        }, ...
],
    "exceedCountDetected": {
        "countPerLayer": {
        ...,
            "layer-2": whether-node-count-for-layer-2-exceeds-the-upper
-limit,
            "layer-1": whether-node-count-for-layer-1-exceeds-the-upper
-limit,
            "layer0": whether-node-count-for-layer0-exceeds-the-upper-l
imit,
            "layer1": whether-node-count-for-layer1-exceeds-the-upper-l
imit,
            "layer2": whether-node-count-for-layer2-exceeds-the-upper-l
imit,
            ...
         },
        "linkCount": whether-node-relationship-count-exceeds-the-upper-
limit
    },
    "messageId": message-ID,
    "message":message
}
```

Parameters

`type`

Specify the type of the link information that you want to retrieve, among the link information types applied to the system.

`type` describes a grouping of relations that have the same meaning. On the **Related node** tab in the Integrated Operation Viewer window, you can filter relations to display only those belonging to a specific type.

For relations within a JP1/IM product or between a JP1/IM product and another product, the following types are used. In addition to these types, the use of user-specified types is also allowed.

- `rootJobnetExecutionOrder`: Relation of the execution order of root jobnets
- `managerAgent`: Relation between the manager and agent of a JP1 product
- `rootJobnetAgent`: Relation between a root jobnet and an AJS agent
- `sameNode`: Relation between nodes with the same name
- `L2Connection`: Relation between layer-2 connection lines managed by JP1/NNMi
- `Infrastructure`: Relation between infrastructure resources managed by JP1/OA
- `monitoringConfiguration`: Relation between a product and a monitoring target in a monitoring product configuration

If this attribute is omitted or it is set to an empty string, the applicable link information is returned regardless of the type of the information.

If this attribute is specified, the link information for the specified type among applicable sets of link information is returned.

`sid`

Specify the SID of the target node. The information on the preceding and succeeding nodes of the specified target is returned.

(Example) When specifying a root jobnet:

`_JP1AJS-M`*JP1/AJS3-manager-host-name*`/_HOST`*JP1/AJS3-manager-host-name*`/`
`_JP1SCHE_`*scheduler-service-name*`/_JP1JOBG_`*job-group-name*`_JP1ROOTJOBNET_`*node-name*

Omitting this parameter causes all link information to be retrieved.

`fromLayerCount`

Specify the maximum number of layers of the preceding node to be retrieved, in the range of `0` to `2147483647`.

If `sid` is specified, the `fromLayerCount` parameter cannot be omitted.

If `sid` is omitted, the value specified for the `fromLayerCount` parameter is ignored.

If the same node exists in more than one layer in link information, the number of layers can exceed the specified value depending on how layers are interpreted.

If this can cause a problem, check whether the excess occurs while retrieving link information before using it.

`toLayerCount`

Specify the maximum number of layers of the succeeding node to be retrieved, in the range of `0` to `2147483647`.

If `sid` is specified, the `toLayerCount` parameter cannot be omitted.

If `sid` is omitted, the value specified for the `toLayerCount` parameter is ignored.

If the same node exists in more than one layer in link information, the number of layers can exceed the specified value depending on how layers are interpreted.

If this can cause a problem, check whether the excess occurs while retrieving link information before using it.

`countPerLayer`

Specify the maximum number of nodes to be retrieved for each node layer, in the range of `1` to `2147483647`.

If `sid` is specified, the `countPerLayer` parameter cannot be omitted.

If `sid` is omitted, the value specified for the `countPerLayer` parameter is ignored.

If the same node exists in more than one layer in link information, the number of layers can exceed the specified value depending on how layers are interpreted.

If this can cause a problem, check whether the excess occurs while retrieving link information before using it.

`linkCount`

Specify the maximum number of node-node relationships (the number of pairs of preceding and succeeding nodes) to be retrieved, in the range of 1 to 2147483647.

If sid is specified, the linkCount parameter cannot be omitted.

If sid is omitted, the value specified for the linkCount parameter is ignored.

If the same node exists in more than one layer in link information, the number of layers can exceed the specified value depending on how layers are interpreted.

If this can cause a problem, check whether the excess occurs while retrieving link information before using it.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	None	There is no data that has not been returned because of the upper limit restriction.
	KAJY22000-W	There is data that has not been returned because of the upper limit restriction.
`400`	KAJY22002-E	The request has a parameter with an invalid format. (The key does not exist or specification and data type are different)
`500`	KAJY22002-E	The request has a parameter with an invalid format. (The value is invalid.)

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response body if the status code is `200`:

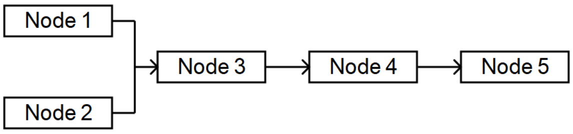
No.	Member name	Data type	Description
1	`links`	array	An array of response objects. The order of the array is irrelevant.
2	`from`	string	The preceding node. The format is the same as that of `sid` in the message body.
3	`to`	string	The succeeding node. The format is the same as that of `sid` in the message body.

No.	Member name	Data type	Description
4	type	string	The same value as type of the request parameter.
5	exceedCountDetected	object	Whether the specified upper limit for a parameter is exceeded. Each parameter has members. If sid is not specified, none is returned.
6	countPerLayer	boolean	Whether the number of nodes per layer exceeds the upper limit. Each layer has members.
7	layer*integer*	string	Whether the number of nodes per layer exceeds the upper limit (for all the target layers). A number is assigned to *integer* as follows: 0 for the layer specified as sid, +1 for the succeeding layer, and -1 for the preceding layer. The number is incremented by one for further succeeding layers, and decremented by one for further preceding layers.
8	linkCount	boolean	Whether the number of links exceeds the upper limit. • true: Exceeded • false: Not exceeded
9	messageId	string	The message ID. This is returned only if there is a message to be notified.
10	message	string	The message body. The used language is determined by the value specified for the Accept-Language property in the HTTP request header. This is returned only if there is a message to be notified.

Example 1

The example below executes the API in the following scenario:

- Identifiers for the target system
  - JP1/AJS3 manager host name: host1
  - Scheduler service name: scheduler1
  - Job group name: jobgroup1
  - Node name: rootjobnet3
- The number of layers of the preceding node to be retrieved: 100
- The number of layers of the succeeding node to be retrieved: 1
- The number of nodes to be retrieved per node layer: 100
- The number of node relationships to be retrieved: 100
- The relationship between nodes:



- Language used in messages: English

Request:

```
POST /im/api/v1/links 1.1
Authorization: Bearer XXXX
Accept-Language: ja
Content-Type: application/json
Accept: application/json
{
    "type": "rootJobnetExecutionOrder",
    "sid": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler1/_JP1JOBG_jo
bgroup1/_JP1ROOTJOBNET_rootjobnet3",
    "fromLayerCount": 100,
    "toLayerCount": 1,
    "countPerLayer": 100,
    "linkCount": 100
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "links": [
        {
        "from": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler2/_JP1JO
BG_jobgroup3._JP1ROOTJOBNET_rootjobnet1",
        "to": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler1/_JP1JOBG
_jobgroup1/_JP1ROOTJOBNET_rootjobnet3",
"type": "rootJobnetExecutionOrder"
        },
        {
        "from": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler4/_JP1JO
BG_jobgroup3/_JP1ROOTJOBNET_rootjobnet2",
        "to": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler1/_JP1JOBG
_jobgroup1/_JP1ROOTJOBNET_rootjobnet3",
        "type": "rootJobnetExecutionOrder"
        },
        {
        "from": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler1/_JP1JO
BG_jobgroup1/_JP1ROOTJOBNET_rootjobnet3",
        "to": "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_scheduler1/_JP1JOBG
_jobgroup2/_JP1ROOTJOBNET_rootjobnet4",
        "type": "rootJobnetExecutionOrder"
        }
        ],
        "exceedCountDetected": {
            "countPerLayer": {
                "layer-1": false,
                "layer0": false,
                "layer1": false,
                 },
        "linkCount": false
    },
    "messageId": "KAJY22000-W",
    "message": "There is data that is not displayed because the upper l
imit is reached. (item = succeeding node layer count)"
}
```

5.5.2 Link type list acquisition

Description

Gets the list of types of link information applied to the system.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
GET /im/api/v1/links/types httpVersion
```

Response message body

```
{
    "linkTypes": [
    {
        "name":"type-of-link-information"
    }
}
```

Parameters

None

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	None	The list of link information types was retrieved successfully.
403	KAJY01000-E	There is no permission to run the REST API.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name		Data type	Description
1	linkTypes		Object[]	An array of link type objects
2		name	string	The SID of the preceding node

Example

Request:

```
GET /im/api/v1/links/types HTTP/1.1
Authorization:Bearer xxxx
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
    "linkTypes": [
        {
            "name":"rootJobnetExecutionOrder"
        },
        {
            "name":"sameNode"
        },  ...
    ]
}
```

5.6 API for event management

This section describes operations for API of event management.

5.6.1 Event search

Description

Get events which related events to IM management node from the integrated monitoring database.

Specifying an IM management node as a parameter returns a list of events that were issued from the node.

Specifying search conditions as a parameter returns a list of events that match the conditions.

Events cannot be retrieved if the logged-in JP1 user has no permission to view the events. Note that such a case causes no error.

What kind of events you can get depends on the JP1 resource group settings and the event receiver filter settings in JP1/IM - Manager.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/treeInfo/event httpVersion
```

Request message body

```
{
    "sid":"tree-SID-of-the-IM-management-node",
    "filter":"event-search-condition",
    "direction":"direction-of-the-event-search",
    "since":"start-position-of-the-event-search",
    "count":"number-of-events-to-be-obtained",
    "attrs":"list-of-event-attributes-to-be-obtained",
    "statusFilter":"statusFilter",
    "consolidateEvent":"whether-to-return-consolidated-repeated-events
",
    "searchCount":"number-of-event-searches"
}
```

Response message body

```
{
  "eventData":[
    event-information-object, ...
  ],
  "messageId":"message-ID",
  "message":"message",
  "beginSid":"next-event-SID-at-the-start-position-of-the-JP1-event-sea
rch",
  "endSid":"event-SID-at-the-end-position-of-the-JP1-event-search"
}
```

Parameters

`sid`

Specify the tree SID of the IM management node as string type.

Obtains the list of events that occurred from the specified IM management nodes. If the parameter is omitted, it is assumed that all systems (`_ROOT_AllSystems`) is specified. Returns an empty list of events if you omit this parameter when the IM management nodes have not been set up.

`filter`

Specify the event search condition object, which stores arrays of conditions.

The system searches the integrated monitoring database for events based on the specified event search conditions. For details on the event search object, see *7.2.1(3) Event search condition object*.

Narrow down the events of that are the target of the `sid` parameter using the event search conditions specified the `filter` parameter.

`direction`

Specify in which direction the event search proceeds.

- Into the past: `past`
- Into the future: `future`

Omitting this parameter causes `past` to be used.

`since`

Specify the SID of the JP1 event that serves as a starting point for the event search. The API searches for events that occurred either before or after the JP1 event corresponding to the specified SID. Note that the JP1 event corresponding to the specified SID is not included in the search.

If this parameter is omitted, the search will be started from the beginning or end of the integrated monitoring database according to the `direction` parameter.

For details on the JP1 event SID, see *7.2.1(1) Event information object*.

`count`

Specify the maximum number of events to be retrieved in the range of `1` to `2000`. Omitting this parameter causes the maximum number to be set to `2000`.

`attrs`

Specify an array of event attributes that you want to get. The attributes specified in this parameter are retrieved in user-specified order.

Example

```
"attrs":["B.ID","B.MESSAGE",...]
```

If this parameter is omitted, all the attributes that can be output by the output of event report functionality and the attributes listed in the table of *Event attributes of the consolidation start event* in *7.2.1(1) Event information object* are retrieved.

For details of the event report functionality, see *4.15.2 Saving event information in the integrated monitoring database (CSV report)* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

`statusFilter`

When I perform narrowing of the status of the IM management node only by an applicable event, I appoint a value of the status with sequence of `int`.

For details of status of IM management node, see *5.8.5 IM management node status acquisition*.

Example: If you want to obtain the events of which the statuses are `30` or `40`.

`"statusFilter":[30,40]`

`consolidateEvent`

Specify whether to return consolidated repeated events when repeated events are consolidated. Omitting this parameter causes the parameter to be set to `false`. If you do not want repeated events to be returned, specify `true`.

- `true`: If repeated-event display is suppressed with the Intelligent Integrated Management Base, only consolidation start events are returned. Repeated events after the consolidation start event are not returned.
- `false`: Repeated events are returned regardless of whether repeated-event display is suppressed with the Intelligent Integrated Management Base.

`searchCount`

Specify the upper limit for the number of event searches from 0 to 120,000.

Up to 100 events mapped with the IM management node specified by the `sid` parameter are searched for, starting from the search start position specified by the `since` parameter in the search direction of the `direction` parameter. If the number of events specified by the `count` parameter cannot be retrieved due to a reason such as an event receiver filter, the next 100 events are repeatedly searched for as the target. Specify the upper limit for the number of these repeated event searches.

If the number of searches reaches the upper limit, the search operation is suspended and the list of events retrieved successfully before the search ends is returned. If the parameter is omitted or if the value is set to `0`, there will be no upper limit for the number of searches.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	None	A list of events was retrieved successfully.
	KAJY32005-W	A temporary error occurred during the event search.
	KAJY32010-W	Event retrieval was suspended because the event search to obtain events reaches the specified upper limit for the number of searches.
`400`	KAJY32200-E	The request has a parameter with an invalid format.
	KAJY32201-E	The event search conditions (the `filter` parameter) are invalid.
`404`	KAJY32202-E	The specified node does not exist on the manager.
`500`	KAJY32000-E to KAJY32004-E KAJY32006-E	An error occurred during the event search process.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`eventData`	Object[]	Returns an array of the event information objects that represents a list of retrieved events. For details on the event information object, see *4.2.2(1) Event information object*. If there is no event to be returned, a zero-length array is returned.

No.	Member name	Data type	Description
2	messageId	string	Returns the message ID of the temporary error message that is generated during an event search. If there is no message to be notified, this information is not returned.
3	message	string	Returns the body of the temporary error message that is generated during an event search. If there is no message to be notified, this information is not returned.
4	beginSid	string	Returns the next JP1 event SID at the start position of the event search. It is the next JP1 event SID in the direction of event retrieval starting from `since`. It is omitted if there is no event to be searched for.
5	endSid	string	Returns the JP1 event SID at the end position of the event search. If event search is suspended, the JP1 event SID at the suspended position is returned. It is omitted if there is no event to be searched for.

Example 1

The following example uses this API to get a list of events that are related to a JP1/AJS job group.

```
POST /im/api/v1/nodes/treeInfo/event HTTP/1.1
Authorization:Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json

{
    "sid": "_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HOST_host
1/_CATEGORY_Job/_SUBCATEGORY_JP1%2FAJS3%20-%20Manager/_OBJECT_ScheduleServ
/_OBJECT_jobgroup",
"count": "200",
"attrs": [ "B.ID","E.@JP1IM_DEALT","E.SEVERITY" ]
}
```

Example 2

The following example uses this API to get a list of events by specifying event search conditions.

Request:

```
POST /im/api/v1/nodes/treeInfo/event HTTP/1.1
Authorization:Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json

{
    "filter": {
        "include": [
            [
            {"key":"E.SEVERITY","ope":"IN","val": ["Error","Warning"]
},
             {"key":"B.SOURCESERVER","ope":"IN","val":["host1","host2",
"host3"]}
            ],
            [
            {"key":"E.SEVERITY","ope":"IN","val": ["Error","Warning","N
otice"] },
            {"key":"B.SOURCESERVER","ope":"IN","val":["host4","host5"]}
            ]
        ],
        "exclude": [
            [
                {"key":" E.@JP1IM_DEALT","ope":"IN","val":"1"}
            ]
        ]
    }
}
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
    "eventData": [
    {
        "sid": "_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IMEVBSEQNO_746",
        "value": [
            "B.ID": "00004107",
            "E.@JP1IM_DEALT": "0",
            "E.SEVERITY": "Error"
    },
    {
        "sid": "_JP1IM_imhost1/_JP1IMSEQNO_698/_JP1IMEVBSEQNO_747",
        "value": [
            "B.ID": "00004104",
            "E.@JP1IM_DEALT": "0",
            "E.SEVERITY": "Error"
    }
    ]
}
```

5.6.2 Event detailed information acquisition

Description

Gets the details of a specified event.

The details of an event cannot be retrieved if the logged-in JP1 user has no permission to view the event.

The retrieved details of an event can include the attributes of the event, the event guide information, and the display names of the event attributes.

Event attributes and their display names to be included in the retrieved details of an event depend on the JP1/IM - Manager definition file for extended event attributes.

If the event guide information is set on JP1/IM - Manager, the event guide message for the retrieved event is included.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator

- JP1_Console_User

API version

v1

Format

Request line

```
GET /application/component/apiVersion/events/detail?query httpVersion
```

Response message body

```
{
    "eventData":event-information-object
}
```

Parameters

sid

Specify the SID of a JP1 event for which you want to get details. For details on the SID of a JP1 event, see *7.2.1(1) Event information object*.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	None	The details were retrieved successfully.
400	KAJY32210-E	The request has a parameter with an invalid format.
404	KAJY32211-E	The specified event could not be found.
500	KAJY32000-E to KAJY32003-E KAJY32005-E to KAJY32008-E	An error occurred during the retrieval of details.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response body if the status code is 200:

No.	Member name	Data type	Description
1	eventData	object	Returns the event information object. For details, see *7.2.1(1) Event information object*.

Example 1

The following example uses this API to get the details of a specified event.

Request:

```
GET /im/api/v1/events/detail?sid=_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IME
VBSEQNO_746 HTTP/1.1
Authorization:Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json
{
  "eventData": {
    "sid": "_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IMEVBSEQNO_746",
    "value": [
      "B.ID":"00001F20",
      "B.MESSAGE":"An error occurred.",
      "E.STARTTIME":"2018-11-14T17:00:00Z",
      "E.@JP1IM_GUIDE":" Check the host1 host for an error.",
         ...
    ],
    "title": [
      "B.ID":"Event ID",
      "B.MESSAGE":"Message",
      "E.STARTTIME":"Start time",
      "E.@JP1IM_GUIDE":"Guide",
          ...
    ],
    "type": [
      "B.MESSAGE":"text",
      "E.STARTTIME":"date",
      "E.@JP1IM_GUIDE":"html",
          ...
    ]
}
```

5.6.3 Event status change

Description

Changes the event status of the specified events.

An error is issued if the logged-in JP1 user has no permission to view the specified events.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator

API version

v1

Format

Request line

```
POST /application/component/apiVersion/events/status httpVersion
```

Request message body

```
{
    "dealt":"event-status"
    "sid":[
         "JP1-event-SID",...
}
```

Response message body

```
{
    "eventData":[
        event information object,...
    ],
    "messageId":massageID,
    "message":massage
}
```

Parameters

`dealt`

Specify one of the following values for a state to which you want to change the event status:

- `0`: Unprocessed
- `1`: Processed
- `2`: Processing
- `3`: Held

`sid`

Specify an array containing the SIDs of events whose status you want to get. For details on the event SID, see *7.2.1(1) Event information object*. You can specify up to 2,000 event SIDs.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	None	The event status was changed successfully.
	KAJY32110-W	Some events were not able to be handled due to insufficient permission.
`400`	KAJY32220-E	The request has a parameter with an invalid format.
`500`	KAJY32100-E to KAJY32109-E	An error occurred while the event status was being changed.
	KAJY32221-E	Cannot be executed due to a change to the event status.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`eventData`	Object[]	Returns the list of events of which statuses were modified as the array of event information objects. For details, see *7.2.1(1) Event information object*. Returns the event for which the operation was correctly performed if some of the events could not be operated due to an inadequate permission.
2	`messageId`	string	Returns the message ID of the temporary error message that occurred during the modification of the statuses. This is returned only if there is a message to be notified.

No.	Member name	Data type	Description
3	message	string	Returns the body text of the temporary error message that occurred during the modification of the statuses. This is returned only if there is a message to be notified.

Notes

- The concurrent execution of a large number of event status change APIs can lead to the degradation of manager performance or cause the manager to time out.
- Before incorporating the execution of the event status change API into your operation, carefully examine how the resulting operation can affect API execution performance and manager performance to ensure that your operational needs are not compromised.

Examples

The following example uses this API to change the event status of specified events to *Processed*.

Request:

```
POST /im/api/v1/events/status HTTP/1.1
Authorization:Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
{
    "dealt": "1",
    "sid":[
    "_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IMEVBSEQNO_746",
    "_JP1IM_imhost1/_JP1IMSEQNO_698/_JP1IMEVBSEQNO_747",
    ]
}
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
  "eventData": [
    {
      "sid": "_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IMEVBSEQNO_746",
      "value": [
        "E.@JP1IM_DEALT": "1"
      ]
    },
    {
      "sid": "_JP1IM_imhost1/_JP1IMSEQNO_698/_JP1IMEVBSEQNO_747",
      "value": [
        "E.@JP1IM_DEALT": "1"
      ]
    }
  ]
}
```

5.6.4 Event generation

Description

Issues the specified JP1 event and registers it with the manager host (local host). After the registration, the serial number of the issued event is returned.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/events/send httpVersion
```

Request message body

```
{
    "eventId": event-ID,
    "message": message,
    "attrs": {extended-attribute-name:extended-attribute-value[, ...]}
}
```

Response message body

```
serial-number-of-the-issued-event
```

Parameters

`eventId`

A basic part event ID to be issued.

Specify it in the following range:

- `0` to `1FFF`
- `7FFF8000` to `7FFFFFFF`

If a value is out of specifiable range, the `KAJY02047-E` message is output.

Omitting this parameter causes `eventId` to be set to `0`.

`message`

Specify message text that describes the JP1 event as a string of 1,023 bytes or smaller. If a string of 1,024 bytes or larger is specified, an exception occurs to exit the process.

Note that the character code of the registered message depends on that of the OS environment in which the manager is located.

`attrs`

An extended attribute.

If the same extended attribute name is specified multiple times, this parameter is overwritten by the value of the last specified extended attribute.

Specify the extended attribute name with a string of up to 32 bytes consisting of alphanumeric characters and underscores (starting with an alphabetic letter and having all capital alphabetic letters). If an extended attribute name that contains any unspecifiable string is specified, the KAJY02047-E message is output. In addition, do not use the prefix E. in the extended attribute name. If E. is specified, the KAJY02047-E message is output.

The total length of all the extended attribute values you can specify is 10,000 bytes.

The following table lists and describes the event attributes registered by the event registration function.

Table 5–13: List of event attributes registered by the event registration function

No.	Category	Item name	Attribute name	Description of the event attribute value
1	Basic attribute	Serial number	SEQNO	Serial number of the JP1 event to be issued
2		Event ID[#1]	ID	Event ID passed through the parameter
3		Registered reason	REASON	Reason why the event was registered in the current server: • 1: The event was issued to the local event server on the current event server. • 2: The event was issued from the current server to a different server (the value cannot be obtained). • 3: The event was issued from a different server to the current server. • 4. The event was transferred from a different server due to the environment setting.
4		Source process ID	PROCESSID	Process ID of the source API
5		Registered time	TIME	Registration time on the source event server
6		Arrived time	ARRIVEDTIME	Registration time on the local event server
7		Source user ID	USERID	User ID of the source process (Fixed value: -1)
8		Source group ID	GROUPID	Group ID of the source process (Fixed value: -1)
9		Source user name	USERNAME	User name of the source process In Windows: SYSTEM, In Linux: root
10		Source group name	GROUPNAME	Group name of the source process (Fixed value: Null string)
11		Event source server name	SOURCESERVER	Source event server name. If the source server name is not specified, the local host is specified.
12		Source IP address	SOURCEIPADDR	IP address of the source event server
13		Destination IP address	DESTIPADDR	Name of a different event server if the source API clearly specifies transfer to a different event server.
14		Source serial number	SOURCESEQNO	Serial number on the source host
15		Code set	CODESET	Stores the character code specified for the OS.
16		Message	MESSAGE	String that describes the JP1 event
17		Detailed event information	BASIC	Detailed information on a basic event attribute
18		AOM information	AOM	AOM information of the event
19	Extended attribute	Original severity level	SEVERITY	The following strings to represent severity, etc.: • "Emergency": Urgent

No.	Category	Item name	Attribute name	Description of the event attribute value
	(common information)#2			• "Alert" : Alert • "Critical" : Critical • "Error" : Error • "Warning" : Warning • "Notice" : Notice • "Information" : Informative • "Debug: Debug
20		User name	`USER_NAME`	Name of the execution user
21		Product name	`PRODUCT_NAME`	Name of the program that issued the JP1 event It can be one of the following program names: • "/HITACHI/JP1/AJS" • "/HITACHI/JP1/AOM" • "/HITACHI/JP1/IM" • "/HITACHI/JP1/NBQ" • "/HITACHI/JP1/NETMDM" • "/HITACHI/JP1/NPS" • "/HITACHI/JP1/NQSEXEC"
22		Object type	`OBJECT_TYPE`	One of the following strings that indicate the object type, etc.: • "JOB" • "JOBNET" • "ACTION" • "ACTIONFLOW" • "PRINTJOB" • "PRINTQUEUE" • "PRINTER" • "BATCHQUEUE" • "PIPEQUEUE" • "JOBBOX" • "LOGFILE" • "LINK" • "SERVICE" • "PRODUCT" • "CONFIGRATION" • "SERVER"
23		Object name	`OBJECT_NAME`	Name of an object, such as a job or jobnet. An element at the bottom layer for a hierarchical object, such as a jobnet
24		Root object type	`ROOT_OBJECT_TYPE`	Type of an object
25		Root object name	`ROOT_OBJECT_NAME`	Name that acts as a unit of directing execution on user operation
26		Object ID	`OBJECT_ID`	Object ID String that can be combined with `PRODUCT_NAME` to uniquely identify the instance of an object within the integrated system
27		Occurrence	`OCCURRENCE`	String that represents an event which occurred on `OBJECT_NAME`, such as:

No.	Category	Item name	Attribute name	Description of the event attribute value
				• "ACTIVE": Active • "INACTIVE": Inactive • "START": Start • "END": End • "NOTSTART": Failed to start • "CANCEL": Canceled • "LATESTART": Scheduled start time has passed • "LATEEND": Scheduled end time has passed • "SUBMIT": Submitted • "ENQUEU": Enqueued • "DEQUEU": Dequeued • "PAUSE": Paused (suspended) • "RELEASE": Paused (resumed) • "RESTART": Restarted • "CREATE": Created • "DELETE": Deleted • "MODIFY": Updated • "RETRY": Retry started • "STOP": Stopped • "MOVE": Moved • "COPY": Copied • "NOTICE": Noticed • "REPLY": Replied • "CONNECT": Connected • "DISCONNECT": Disconnected • "EXCEPTION": Error other than the above
28		Start time	`START_TIME`	Time execution started or re-execution started
29		End time	`END_TIME`	Time execution ended or re-execution ended
30		Result code	`RESULT_CODE`	Result code
31		Event source host name	`JP1_SOURCEHOST`	Is set to `B.SOURCESERVER` if an event source host name is not specified
32		Individual extended attribute count	Individual extended attribute count	Number of extended attributes

#1

The following shows the format for database output:

Example: `ID:IDEXT 0000000A:00000000`

#2

Common attributes are stored in an array. They are not registered if not specified.

The following shows the attribute values of an event registered by this REST API:

-- This parameter is used for execution

```
{
   "eventId":"10000",
   "message":"A failure occurred in the cloud service",
   "attrs":{"SEVERITY":"Error"}
```

```
}
SQ 18840099
ID 00010000:00000000
KN 0
HD 0
PI 0
RT 1559790829
AT 1559790829
RR 1
UI -1
GI -1
HQ 18840099
UN jp1admin
GN
SN HOSTA
SI %0Aﾜﾄ(
CS MS932
MS A failure occurred in the cloud service
UP %00%00%00%00%00%00%00%00
XN 1
XV SEVERITY= Error
```

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	None	A JP1 event was issued.
400	KAJY02047-E	The format of the parameter specified for the request is invalid.
403	KAJY01000-E	There is no permission to run the REST API.
500	KAJY02048-E	A JP1 event could not be issued.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

The following information is returned in the response body if the status code is `200`:

Data type	Description
Number	Serial number of an issued event

Examples

The following shows a usage example of the event API:

Request:

```
POST http://hostname:20703/im/api/v1/events/send
{
  "eventId":"1FFF",
  "message":"A failure occurred in Service A",
  "attrs":{"SEVERITY":"Error","JP1_SOURCEHOST":"HOSTA"}
}
```

Response:

```
18839936
```

5.6.5 JP1 Event converter

Description

The event information notified by the external system is converted into a JP1 event and issued.

The event information notified by the external system is passed to the product plug-in, and the JP1 event is issued according to the returned JP1 event information.

Execution permissions

None

API version

v1

Format

Request line

```
POST /im/api/v1/events/transform HTTP/1.1
```

Request header

Header name	Setting value
`Authorization`	Do not set it.

If message body of the request is in JSON format, the other request headers are the same as Common spec of API. For the request header of Common spec of API, see the explanation of the request header in *5.2.3 Request format*.

Request message body

You can send it in JSON format. The data structure of the object is arbitrary (using the unique format of each product plug-in).

JP1/IM - For all product plug-ins set in Manager, if the data cannot be converted to JP1 events, try to convert to JP1 events in the following format.

```
[
    {
        "eventId":event ID,
        "message":messag,
        "attrs":{extended attribute name:extended attribute value, ...}
    },
    ...
]
```

Response message body

```
{
    "eventSeqNo":[Serial number in the DB of the issued event, ...]
    "exceeddJp1eventMaxDetected":Detection of exceeding the upper limi
t of the number of converted JP1 events,
    "messages":[
        {
            "messageId":"Message ID",
            "message":"message body"
        },
        ...
    ]
}
```

Parameters

Here are the parameters that you specify for message body of the request:

No.	Parameters	Data type	Description
1	eventId#	string	Specifies the event ID to be published.
2	message#	string	Specifies the message text that describes the content of the event.
3	attrs#	Array	Specifies extended attributes.

Note #

For details on the contents to be specified for each item, see the parameters of *5.6.4 Event generation*.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API processing succeeded.
	KAJY67002-W	Communication with JP1/Base Events Service failed.
	KAJY67003-W	More than 100 JP1 events were converted.
	KAJY67000-W	The retrieved data did not contain the event ID.
		The retrieved data did not contain a message.
		Invalid extension attribute specification.
		The extended attribute name exceeds 32 bytes.
		The sum of the extended attribute values exceeds 10000 bytes.
406	KAJY67001-E	The JP1 event data was not returned from each linked product plug-in, and the data format was not the default format.

The following information with JSON format is returned in the response body if the status code is 200:

No.	Member name	Data type	Description
1	eventSeqNo	Object[]	Returns the DB serial number of the issued event as a string type array.
2	exceedJp1eventMaxDetected	boolean	Whether or not it is detected that the number of converted JP1 events has exceeded the upper limit. • true: Detected • false: Do not detect
3	messages	object[]	An array of messages to be notified. If there is no message to be notified, it is omitted.
4	messageId	string	The message ID. If there is no message to be notified, it is omitted.
5	message	string	The message body. The language used is determined by the Accept-Language property specified in the HTTP request header. If there is no message to be notified, it is omitted.

Examples

The following is an example of using this API using the OSS curl command.

```
>curl -i --header "Accept-Language: ja" --header "Content-Type: applicatio
n/json" --request POST --data @c:\\work\\request.json "http://localhost:20
703/im/api/v1/events/transform"
```

request.json

```
{
  "receiver":"JP1IMDD",
  "status":"firing",
  "alerts":
  [
    {
      "status":"firing",
      "labels":
      {
        "alertname":"jp1_pc_exporter_healthcheck",
        "instance":"win2016:20717",
        "job":"jpc_windows",
        "jp1_pc_eventid":"0002",
        "jp1_pc_exporter":"JPC Windows exporter",
        "jp1_pc_metricname":"up",
        "jp1_pc_nodelabel":"Windows exporter",
        "jp1_pc_product_name":"/HITACHI/JP1/JPCCS",
        "jp1_pc_prome_hostname":"win2016",
        "jp1_pc_severity":"Error"
      },
      "annotations":
      {
        "jp1_pc_description":"Exporter is down."
      },
      "startsAt":"2021-12-17T07:46:20.027Z",
      "endsAt":"0001-01-01T00:00:00Z",
      "generatorURL":"http://win2016:20713/graph?g0.expr=up%7Bjp1_pc_re
mote_monitor_instance%3D%22%22%7D+%3D%3D+0+or+label_replace%28sum+by%28
jp1_pc_remote_monitor_instance%2C+jp1_pc_exporter%29+%28up%7Bjp1_pc_rem
ote_monitor_instance%21%3D%22%22%7D%29%2C+%22jp1_pc_nodelabel%22%2C+%22
%24%7B1%7D%22%2C+%22jp1_pc_remote_monitor_instance%22%2C+%22%5E%5B%5E%3
A%5D%2A%3A%28%5B%5E%3A%5D%2A%29%24%22%29+%3D%3D+0\u0026g0.tab=1",
      "fingerprint":"430af6034503a24d"
    }
  ],
  "groupLabels":
  {
    "alertname":"jp1_pc_exporter_healthcheck",
    "instance":"win2016:20717",
    "job":"jpc_windows",
    "jp1_pc_eventid":"0002",
    "jp1_pc_exporter":"JPC Windows exporter",
    "jp1_pc_metricname":"up",
    "jp1_pc_nodelabel":"Windows exporter",
    "jp1_pc_product_name":"/HITACHI/JP1/JPCCS",
    "jp1_pc_prome_hostname":"win2016",
    "jp1_pc_severity":"Error"
  },
  "commonLabels":
  {
    "alertname":"jp1_pc_exporter_healthcheck",
    "instance":"win2016:20717",
    "job":"jpc_windows",
    "jp1_pc_eventid":"0002",
    "jp1_pc_exporter":"JPC Windows exporter",
    "jp1_pc_metricname":"up",
    "jp1_pc_nodelabel":"Windows exporter",
    "jp1_pc_product_name":"/HITACHI/JP1/JPCCS",
    "jp1_pc_prome_hostname":"win2016",
    "jp1_pc_severity":"Error"
  },
  "commonAnnotations":
  {
    "jp1_pc_description":"Exporter is down."
  },
  "externalURL":"http://win2016:20714",
  "version":"4",
  "groupKey":"{}:{alertname=\"jp1_pc_exporter_healthcheck\", instance=\
"win2016:20717\", job=\"jpc_windows\", jp1_pc_eventid=\"0002\", jp1_pc_
exporter=\"JPC Windows exporter\", jp1_pc_metricname=\"up\", jp1_pc_nod
elabel=\"Windows exporter\", jp1_pc_product_name=\"/HITACHI/JP1/JPCCS\"
, jp1_pc_prome_hostname=\"win2016\", jp1_pc_severity=\"Error\"}",
  "truncatedAlerts":0
}
```

Example of response:

```
{"eventSeqNo":["19"],"exceedJp1eventMaxDetected":false}
```

5.7 API for plug-ins

This section describes the API for plug-ins.

5.7.1 Plug-in processing execution

Description

Executes any functional operation for a plug-in.

Execution permissions

See *Appendix E.1 Operating permissions required for system monitoring using the Intelligent Integrated Management Base* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

If you specify `_performanceDataGet` for the method parameter when JP1/PFM is linked, the `Admin` or `Operator` permissions must be granted to the execution user for the resource group of the JP1/PFM agent.

API version

v1

Format

Request line

```
POST /application/component/apiVersion/actions httpVersions
```

Request message body

```
{
    "method": function-name,
    "sid": target-IM-management-node-SID,
    "args": operation-specification
}
```

Response message body

```
result-of-the-operation
```

Parameters

`method`

Specify the name of the plug-in function to execute. A function name starting with double underscores (__) is not allowed.

The following function is provided by default:

Function name	Plug-in	Operation
`_performanceDataGet`	JP1/PFM plug-in	Getting performance information

`sid`

Specify the IM management node to be operated with the plug-in, in the SID format of configuration information. Only the IM management node at the end of the system configuration tree can be specified.

For details on the SID, see *7.1 SID*.

`args`

Specify the values to pass to the `args.methodArgs` argument of the plug-in function to execute. If there is no information to be passed, specify an empty object (`{}`).

The size of specified values must be less than 10 MB including other parameters.

The following table describes what value is passed to `args.methodArgs` when the `method` parameter is set to `_performanceDataGet`:

No.	Member name	Data type	Optional	Description
1	`recordId`	string	No	Specify the record ID to be retrieved. Only uppercase characters can be used. The prefix of the record ID, `PI_`, `PD_`, or `PL_` can be omitted. For example, if the prefix is `PI_`, you can specify `LOGD` instead of `PI_LOGD`. Note that if another record that has a different prefix but has the same record ID excluding the prefix exists, it is assumed that both records are specified.
2	`fieldIds`	string[]	Yes	Specify the fields you get as an array. Only uppercase characters can be used. If you want to get performance data of specific fields, specify the field IDs# in array format. # The format is *record-ID_PFM-Manager-name*. For `CPU%` of the `PD_PDI` record, the field ID is `PD_PDI_PCT_PROCESSOR_TIME`. If this member is omitted, all the fields in the specified record are output. If an empty value is specified (that is, `fieldIds:[ ]`), it is assumed that this member is omitted. Note that the data below (key field needed to identify the record) is output even if the field ID is omitted. For details on the key fields, see the manual of each agent. - Historical report (single agent) - `"Date and Time"` field - `ODBC` key field
3	`startTime`	string	No	Specify the start date and time of reporting. Use the ISO8601 extended format (*YYYY*-*MM*-*DD*T*hh*:*mm*:*ss*Z). The letter `Z` at the end of the time indicates the UTC timezone. In the timezone other than UTC, use the format of +*hh*:*mm* or -*hh*:*mm*.
4	`endTime`	string	No	Specify the end date and time of reporting. Use the ISO8601 extended format (*YYYY*-*MM*-*DD*T*hh*:*mm*:*ss*Z) for the date and time of the UTC timezone. The letter `Z` at the end of the time indicates the UTC timezone. In the timezone other than UTC, use the format of +*hh*:*mm* or -*hh*:*mm*.
5	`interval`	string	No	Specify the interval of reporting. Use the format below. It is case insensitive. • `MIN`: In minutes • `HOUR`: In hours • `WEEK`: Weekly • `DAY`: Daily • `MONTH`: Monthly • `YEAR`: Yearly The interval is ignored when specified for a PD record.
6	`filter`	object[]	Yes	Specify this member if you want to filter the performance data you get by its field value. Filtering is possible for more than one field. If you specify multiple filter conditions, the system retrieves the performance data that meets all the conditions (AND condition).

No.	Member name	Data type	Optional	Description
				If an empty value is specified (that is, `filter:[ ]`), it is assumed that this member is omitted.
7	`limit`	number	Yes	Specify the maximum number of records to be retrieved. The possible values are from `1` to `4320`. If this member is omitted, it is assumed that the specified value is `4320`. Specifying a value other than permitted values generates an error, causing the operation to stop.

The following table describes the format of the object you specify for `filter`:

No.	Member name	Data type	Optional	Description
1	`fieldId`	string	No	Specify the filter ID of the field to be filtered. Only uppercase characters can be used.
2	`operator`	string	Yes	Specify the filter condition for performance data you get. Select one of the following values: • =: The value of the field is equal to `value`. • <>: The value of the field is not equal to `value`. • <: The value of the field is less than `value`. • <=: The value of the field is less than or equal to `value`. • >: The value of the field is greater than `value`. • >=: The value of the field is greater than or equal to `value`. If this member is omitted, it is assumed that = is specified.
3	`value`	string	No	Specify the value according to the field format described in the manuals for JP1/PFM - Agent or JP1/PFM - RM. Note the following description for the ranges: - Character The specified value is applied as it is. However, `*` is handled as a wildcard character. - Integer An integer must be within the acceptable range of the data type for the field, which is from -2,147,483,648 to 2,147,483,647. However, the check range of the ulong (unsigned long) data type can be extended by specifying the `condExpValueUlongExtension` parameter in `config.xml` for JP1/PFM - Web Console. For details on the `config.xml` parameter, see the *JP1/ Performance Management Reference*. - Decimal number Specify a value within the acceptable range of the data type for the field. If the format of the target field is float or double, and the field value has four decimal places or more, the value is rounded off to the third decimal place. If the format of the target field is utime and the field value has seven decimal places or more, the value is rounded off to the sixth decimal place. For details on the format of the field, see the description of each field in the manuals for JP1/PFM - Agent or JP1/PFM - RM. - Date Specify the date and time in ISO8601 extended format (*YYYY*`-`*MM*`-`*DD*`T`*hh*`:`*mm*`:`*ss*`Z`). The letter `Z` at the end of the time indicates the UTC timezone. In the timezone other than UTC, use

No.	Member name	Data type	Optional	Description
				the format of +*hh*:*mm* or -*hh*:*mm*. (The time always uses the *HH*:*mm*:*ss* format.) Note that an error occurs if any of control characters, (,), [,], <, >, =, and " is contained in the value. The acceptable number of bytes is a maximum of 2,048 bytes.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	None	Plug-in execution succeeded.
400	KAJY22003-E	The request has a parameter with an invalid format.
403	KAJY22004-E	There is no permission to access the specified IM management node.
500	KAJY22005-E	An error occurred during the plug-in processing.

For details on the messages, see the *JP1/Integrated Management 3 - Manager Messages*.

Return values

No.	Member name	Data type	Description
1	--	object	The object in which the execution result of the plug-in processing is stored. The return value of the plug-in function is assigned to the object.

The following table describes the return value when the method parameter is set to _performanceDataGet:

No.	Member name	Data type	Description
1	component	string	Component name This is always set to HITACHI/JP1/PFM/CONFINFO.
2	productId	string	Product ID of the agent whose performance data is to be retrieved
3	dataModelVersion	string	Data model version of the agent whose performance data is to be retrieved
4	rc	number	Return code • 0: Data was retrieved successfully. • 1: Data was retrieved successfully but some records were not retrieved due to limit. • 2: There is no data in the specified period.
5	fields	object[]	Array of field information objects
6	data	string[][]	Two dimensional array of performance data, in [row data] [column data] format. The output order of the column data guarantees the output order of the field information. The data and time data is returned as the data and time in the UTC timezone in ISO8601 extended format (*YYYY*-*MM*-*DD*T*hh*:*mm*:*ss*Z). Any timezone other than UTC is not supported. In addition, if dataType of the output data is one of FOLAT, DOUBLE, or SECTIMEDOUBLE and its value is less than 10 to the negative third power or greater than or equal to 10 to the seventh power, the value is output in floating point format (such as 1.01E10).

The following table describes the format of the field information object:

No.	Member name	Data type	Description
1	`id`	string	Field ID
2	`displayName`	string	Display name of the field
3	`dataType`	string	Data type of the field: • `STR`: String • `SHORT`: 16-bit integer • `INT`: 32-bit integer • `LONG`: 64-bit integer • `FLOAT`: 32-bit single-precision floating-point number • `DOUBLE`: 64-bit double-precision floating-point number • `SECTIMELONG`: Long value that indicates the time (in seconds) since a particular point in time#1 • `SECTIMEDOUBLE`: Double value that indicates the time (in seconds) since a particular point in time#1 • `MILLTIME`: Long value that indicates the time (in milliseconds) since a particular point in time#1 • `DATE`: Data that represents only the year, month, and day (*yyyy*-*MM*-*DD*`T`*hh*`:`*mm*`:`*ss*`Z`) • `DATETIME`: Data that represents the year, month, day, and time (hour, minute, and second) (*yyyy*-*MM*-*DD*`T`*hh*`:`*mm*`:`*ss*`Z`) • `TIME`: Data that represents only the time (*yyyy*-*MM*-*DD*`T`*hh*`:`*mm*`:`*ss*`Z`, only the time is output as the information.)
4	`keyType`	string	Key attribute of the field needed for identifying data (record)#2 • `DATE` It must be specified in one field of all fields, and indicates that the field is a key to identifying the time. • `INST` It is specified in zero or more fields of all fields, and indicates that the field is a key specific to data (record). • `NONE` It indicates that the field is not a key.

#1

The point in time serving as a reference depends on the fields. See each field (field in utime format) of JP1/PFM - Agent or JP1/PFM - RM.

#2

The following table lists the combination of key attributes required to identify the data (record):

Report type	Record type	Combination of attributes required for data identification
Historical report (Single agent)	Single row record	• `DATE`
	Multi-row record	• `DATE` • `INST`

Examples

The example below uses the API in the following scenario:

- The functionality to use: JP1/PFM plug-in for getting performance information
- JP1/PFM manager host name: `mgrhost1`
- JP1/PFM agent host name: `agenthost1`

- Target IM management node: JP1/Performance Management - Agent Option for Platform (For Windows)
- The monitoring item to be retrieved: CPU usage
- Output start time: April 1, 2017 00:00:00 JST
- Output end time: April 1, 2017 01:00:00 JST

Request:

```
POST /im/api/v1/actions HTTP/1.1
Authorization:Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
{
    "method": "_performanceDataGet",
    "sid": "_JP1PFM-M_MGRHOST1/_JP1PFM-AHOST_AGENTHOST1/_HOST_AGENTHOST
1/_JP1PFM-A_TA1agenthost1",
    "args": {
        "recordId": "PI",
        "fieldIds": ["PI_PCT_TOTAL_PROCESSOR_TIME"],
        "startTime": "2017-04-01T00:00:00+09:00",
        "endTime": "2017-04-01T01:00:00+09:00",
        "interval":"HOUR"
    }
}
```

Response:

```
{
    "component": "/HITACHI/JP1/PFM/CONFINFO",
    "productId": "T",
    "dataModelVersion": "8.4",
    "rc": 0,
    "fields": [
    {
        "id": "PI_DATETIME",
        "displayName": "Date and Time",
        "dataType": "DATETIME",
        "keyType": "DATE"
    },
    {
        "id": "PI_PCT_TOTAL_PROCESSOR_TIME",
        "displayName": "CPU %",
        "dataType": "FLOAT",
        "keyType": "NONE"
    }
    ],
    "data": [
        [
            "2017-03-31T15:00:00Z",
            "14.04"
        ],
        [
            "2017-03-31T16:00:00Z","13.55"
        ]
    ]
}
```

5.8 API for system status monitoring

This section describes operations for API of system status monitoring.

5.8.1 IM management node related information generation

Description

Obtain the product-managed configuration from JP1/AJS3, JP1/PFM, JP1/IM and JP1/Base, and use the following file to generate configuration management tree File:

- System node definition file (imdd_systemnode.conf)
- Category name definition file for IM management nodes (imdd_category_name.conf)
- Target host definition file for configuration collection (imdd_target_host.conf)
- Host name definition file (imdd_host_name.conf)

The storage directory of files created by this API is as follows.

In Windows:

- For a physical host:
  Manager-path`\tmp\imdd\imnode\data`
- For a logical host:
  shared-folder`\JP1IMM\tmp\imdd\imnode\data`

In Linux:

- For a physical host:
  `/var/opt/jp1imm/tmp/imdd/imnode/data`
- For a logical host:
  shared-directory`/jp1imm/tmp/imdd/imnode/data`

If the generation is successful, the JP1 event "3F80" is issued, and if the generation fails, the "3F81" is issued.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/create httpVersion
```

Request message body

None

Response message body

For normal termination, there is no response.

For termination with warning, the following response is returned.

```
{
  "returnCode": return-code,
  "messageList":[
    {
      "messageId": message-ID,
      "message": message
    },
    ...
  ]
}
```

Parameters

None

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	`OK`	Success.
`400`	`Bad Request`	The request header is invalid.
`403`	`Forbidden`	You do not have execute permission.
`404`	`Not Found`	No resource.
`406`	`Not Acceptable`	Accept header or Accept-Language header is invalid.
`408`	`Request Timeout`	The request timed out.
`415`	`Unsupported media type`	Content-Type header specification is invalid.
`500`	`Internal Server Error`	The server operation error occurred.
`503`	`Service Unavailable`	Service is not available. The service is temporarily unavailable due to overload or maintenance. It is returned when a temporary error occurs (when it is expected to improve over time).

Return values

Return values	Description
2	Exclusive locking is in progress.
6	Execute of this API does not have enough data.
9	The path of the storage directory is too long.
13	A required file does not exist.
14	A required file could not be read.
15	A required file has an invalid format.
16	A required file has an invalid description.
17	Invalid information was received from the plug-in.
18	Information from the plug-in is invalid.
20	Failed to create IM management node file.
21	Failed to create IM management node link file.

Return values	Description
23	Failed to create IM management node tree file.
26	The user used for authentication has insufficient permissions.
255	The system error.

Examples

The following is a sample API that generates a configuration management tree file:

Request:

```
POST /im/api/v1/nodes/create HTTP/1.1
Authorization: Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJM
E9qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJ
Q0FnSUNBZ0lDQWdJQ0Fn
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json
```

5.8.2 IM management node related information reflection

Description

The following file obtained by the IM Management Node Related Information Generation API and the IM Management Node Link Definition File are used to create the configuration management tree.:

- IM management node tree file
- IM management node data files
- IM management node link file

If the new/rebuild mode is specified as the import method, all JP1 events stored in the integrated management database are acquired and evaluated, and the status of each IM management node is evaluated.

When the configuration change mode is specified for the import method, no JP1 events are acquired from the integrated monitoring DB and IM management node status information and event information related to IM management node that are already retained are inherited for use.

The directory where files created by the IM Management Node Related Information Generation API are stored is as follows.

In Windows:

- For a physical host:
  Manager-path`\tmp\imdd\imnode\`*data*
- For a logical host:
  shared-folder`\JP1IMM\tmp\imdd\imnode\`*data*

In Linux:

- For a physical host:
  `/var/opt/jp1imm/tmp/imdd/imnode/`*data*
- For a logical host:
  shared-directory`/jp1imm/tmp/imdd/imnode/`*data*

In addition, JP1 event "`3F82`" is issued if reflection is successful, and "`3F83`" is issued if reflection fails.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/update httpVersion
```

Request message body

```
{
  "mode": import-method
}
```

Response message body

For normal termination, there is no response.

For termination with warning, the following response is returned.

```
{
  "returnCode": return-code,
  "messageList":[
    {
      "messageId": message-ID,
      "message": message
    },
    ...
  ]
}
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter name	Data type	Optional	Description
`mode`	`string`	Yes	Specify the import method. • `reconfigure` Reflect in the new/rebuild mode. • `change` Reflect in the configuration change mode. By default, it follows setting value of `jp1.imdd.simt.updateMode` property of Intelligent Integrated Management Base definition file (imdd.properties).

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	`OK`	Success.
`400`	`Bad Request`	The request header is invalid.
`403`	`Forbidden`	There is no execution permission.
`404`	`Not Found`	The resource could not be found.
`406`	`Not Acceptable`	An invalid Accept or Accept-Language header is specified.
`408`	`Request Timeout`	The request timed out.
`415`	`Unsupported media type`	An invalid Content-Type header is specified.
`500`	`Internal Server Error`	An error occurred with the server processing.
`503`	`Service Unavailable`	Service is not available. The service is temporarily unavailable due to overload or maintenance. It is returned when a temporary error occurs (when it is expected to improve over time).

Return values

Return values	Description
2	Exclusive locking is in progress.
3	Invalid argument.
6	Execute of this API does not have enough data.
9	The storage directory path is too long.
10	JP1/IM - Manager database service is not running.
13	A required file does not exist.
14	A required file could not be read.
15	A required file has an invalid format.
16	A required file has an invalid description.
17	Failed to get event information.
19	Invalid information was received from the plug-in.
22	Failed to replace master file.
26	The user used for authentication has insufficient permissions.
27	There are suggestion definitions that do not map to any IM management node.
28	Failed to create proposal related master file.
29	Suggestion-related master file replacement failed.
255	The system error.

Examples

Here is a sample API that recreates configuration management tree, retrieves and evaluates all of JP1 events stored in the integrated administration DB, and reflects the status of the configuration objects in the tree that you created.

Request:

```
POST /im/api/v1/nodes/update HTTP/1.1
Authorization: Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJM
E9qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJ
Q0FnSUNBZ0lDQWdJQ0Fn
Accept-Language: ja
Content-Type: application/json
Accept: application/json

{
  "mode":"reconfigure"
}
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json
```

5.8.3 IM management node information acquisition

Description

Gets the IM management node information collected from JP1/AJS3, JP1/PFM, JP1/IM, JP1/Base, and others. It can get all IM management node information, regardless of view permissions of the logged-in JP1 user.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
GET /application/component/apiVersion/nodes/configInfo httpVersion
```

Request message body

None.

Response message body

```
{
    "simtData":[
        IM-management-node-information-object,...
    ]
}
```

Parameters

None.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	OK	The IM management node information was retrieved successfully.
400	Bad Request	The request header is invalid.
401	Unauthorized	Authentication is required.
403	Forbidden	There is no execution permission.
404	Not Found	The resource could not be found.
406	Not Acceptable	An invalid `Accept` or `Accept-Language` header is specified.
412	Precondition failed	The server cannot be accessed.
415	Unsupported media type	An invalid `Content-Type` header is specified.
500	Internal Server Error	An error occurred with the server processing.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	simtData	object[]	Returns an array of the IM management node information objects that contain collected IM management node information. A zero-length array is returned if no IM management node information.

Examples

The following example uses this API to get IM management node information.

Note that the value of the `Authorization` header must be specified in a single line.

Request:

```
GET /im/api/v1/nodes/configInfo HTTP/1.1
Authorization: Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
"simtData":[
    {"sid":"_JP1AJS-M_host1/_HOST_host1","value":{...}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv","value"
:{...}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG
_jobgroup","value":{...}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG
_jobgroup/_JP1ROOTJOBNET_jobnet1","value":{...}},
    {"sid":"_JP1AJS-M_host1/_JP1AJS-A_AGT10/_HOST_host10","value":{...}
},
    {"sid":"_JP1PFM-M_host2/_HOST_host2","value":{...}},
    {"sid":"_JP1PFM-M_host2/_JP1PFM-A_servid/_HOST_host20","value":{...
}}
  ]
}
```

5.8.4 Configuration management tree information acquisition

Description

Gets tree information that is displayed in the status monitoring functionality of the Intelligent Integrated Management Base. IM management node tree information cannot be retrieved if the logged-in JP1 user has no permission to view the tree information.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
GET /application/component/apiVersion/nodes/treeInfo httpVersion
```

Request message body

None.

Response message body

```
{
  "simtData ":[
     IM-management-node-tree-information-object,...
  ]
}
```

Parameters

None.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	OK	The IM management node tree information was retrieved successfully.
400	Bad Request	The request header is invalid.
401	Unauthorized	Authentication is required.
403	Forbidden	There is no execution permission.

Status code	Message	Description
`404`	`Not Found`	The resource could not be found.
`406`	`Not Acceptable`	An invalid `Accept` or `Accept-Language` header is specified.
`412`	`Precondition failed`	The server cannot be accessed.
`415`	`Unsupported media type`	An invalid `Content-Type` header is specified.
`500`	`Internal Server Error`	An error occurred with the server processing.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`simtData`	object[]	Returns an array of IM management node tree information objects that contain collected IM management node tree information. A zero-length array is returned if no IM management node tree information is available. For details on the IM management node tree information object, see *7.2.2(1) IM management node tree object*.

Examples

The following example uses this API to get IM management node tree information.

Note that the value of the `Authorization` header must be specified in a single line.

Request:

```
GET /im/api/v1/nodes/treeInfo HTTP/1.1
Authorization: Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
    "simtData":[
        {"sid":"_ROOT_AllSystems","value":{"target":[],"label":"All Sys
tems"}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1","value":{"target":[],
"label":"System 1",...}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1","v
alue":{"target":[],"label":"Sub system 1",...}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HO
ST_host1","value":{"target":[],"label":"host1",...}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HO
ST_host1/_CATEGORY_Job","value":{"target":[],"label":"Job",...}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HO
ST_host1/_CATEGORY_Job/_OBJECT_JP1AJSMJOB","value":{"target":[],"label"
:"JP1/AJS3 - Manager"}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HO
ST_host1/_CATEGORY_Job/_OBJECT_JP1AJSMJOB/_OBJECT_ScheduleServ","value"
:{"target":[],"label":"ScheduleServ",...}},
        {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HO
ST_host1/_CATEGORY_Job/_OBJECT_JP1AJSMJOB/_OBJECT_ScheduleServ/_OBJECT_
jobgroup","value":{"target":[],"label":"jobgroup",...}},
         {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_H
OST_host1/_CATEGORY_job/_OBJECT_JP1AJSMJOB/_OBJECT_ScheduleServ/_OBJECT
_jobgroup/_OBJECT_jobnet1","value":{"target":[],"label":"jobnet1",...}}
    ]
}
```

5.8.5 IM management node status acquisition

Description

Gets the status information of all IM management nodes (management groups or management objects). If you specify IM management nodes as a parameter, the status information of only the specified IM management nodes is retrieved.

If the IM management node that the logged-in JP1 user has no permission to view is specified, zero-length array is returned.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/treeInfo/status httpVersi
on
```

Request message body

```
{
    "sid":[
    "IM-management-node-tree-SID"., ...
        ]
}
```

Response message body

```
{
    "simtData":[
    status-information-object,...
        ]
}
```

Parameters

`sid`

Specify the tree SID of the IM management node. You can get the status information of the specified IM management nodes. For details on the SID, see *7.1 SID*.

This parameter accepts multiple values.

Omitting this parameter causes the status information of all accessible IM management nodes to be retrieved.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	`OK`	The status of IM management nodes was retrieved successfully.
`400`	`Bad Request`	The request header is invalid.
`401`	`Unauthorized`	Authentication is required.
`403`	`Forbidden`	There is no execution permission.
`404`	`Not Found`	There is no permission to access the resource or the resource is not found.
`406`	`Not Acceptable`	An invalid `Accept` or `Accept-Language` header is specified.
`412`	`Precondition failed`	The server cannot be accessed.
`415`	`Unsupported media type`	An invalid `Content-Type` header is specified.
`500`	`Internal Server Error`	An error occurred with the server processing.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`simtData`	object[]	Returns the retrieved status information as an array of the status information objects. A zero-length array is returned if no IM management node is found for the specified identifier or no IM management node is available.

Definition format

```
{
  simtData: [
    {
      "sid": "SID-of-the-tree",
      "value":{
        "status":{"JP1EVENT": status-value}
      }
    },
    ...
  ]
}
```

Members

The following table describes the members:

No.	Member name	Data type	Description
1	simtData	array	An array that stores the status information
2	sid	string	The SID of the tree for the IM management node
3	value	array	An array that stores the status values
4	status	string	The status of the SID for the IM management node The type of the status (JP1EVENT) and a number that represents the status

Only simtData objects that are on the tree nodes whose status has been changed more than once due to JP1 events or higher-level propagation in the tree nodes specified by the request parameter will be returned.

The status values mean:

- 40: An Emergency-, Alert-, Critical-, or less-severe-level event occurred but was not processed.
- 30: An Error- or less-severe-level event occurred but was not processed.
- 20: A Warning- or less-severe-level event occurred but was not processed.
- 10: All the applicable severe events have been processed (or canceled or removed), and the system is in a healthy condition.

Examples

The following example uses the API to get the status of a management object, which is a jobnet with the SID of _JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jobgroup/_JP1ROOTJOBNET_jobnet1.

Note that the value of the Authorization header must be specified in a single line.

Request:

```
POST /im/api/v1/nodes/treeInfo/status HTTP/1.1
Authorization: Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json

{
    "sid":[
    "_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jobgro
up/_JP1ROOTJOBNET_jobnet1"
    ]
}
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
    "simtData":[
        {
        "sid": "_ROOT_AllSystem",
        "value":{
        "status":{"JP1EVENT": 40}
        }
    ]
}
```

5.8.6 Suggestion mapping information acquisition

Description

Gets the suggestion definition mapping information, which maps the information of the configuration management tree to the suggestion definition information.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
GET /application/component/apiVersion/nodes/treeInfo/suggestions httpVersion
```

Request message body

None.

Request message body

```
{
    "simtData": [
        {
            "sid": tree-SID,
            "value":{
                        "suggestionIds": [suggestion-ID,...]
                    }
            }
        },
        ...
    ]
}
```

Parameters

None.

Status codes

The following table describes the status codes that may be returned as a response to a request:

Status code	Message	Description
200	None	The suggestion definition mapping information was successfully acquired.
403	KAJY01000-E	The logged-in user does not have the permission to execute the REST API.

Return values

The following information is returned in the response body if the status code is 200:

No.	Member name			Data type	Description
1	`simtData`			object[]	Returns the acquired suggestion definition mapping information as an array. However, information of a tree SID to which no suggestion definition is mapped is not returned. When neither the `jddupdatetree` nor `jddupdatesuggestion` command is executed, an empty array is returned.
2		`sid`		string	Specifies the tree SID of the IM management node.
3		`value`		object	Additional information of the tree SID.
4			`suggestionIds`	string[]	An array of the suggestion IDs that are mapped to the tree SID. Even if the logged-in user is not allowed to view some suggestion definitions, the suggestion IDs corresponding to such definitions are returned.

Examples

The following example shows how to use this API:

Request:

```
GET http://hostname:20703/im/api/v1/nodes/treeInfo/suggestions
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "simtData":[
        {"sid":"_ROOT_AllSystems/_HOST_HISOL_host1/_CATEGORY_job/_OBJEC
T_JP1AJSMJOB","value":{"suggestionIds":["suggestion1","suggestion2"]}},
        ...
    ]
}
```

5.9 API for proxy

This section describes operations for proxy.

5.9.1 Proxy credential setup

Description

Sets up credentials of the proxy server when a REST API is executed from a user-created plug-in on the Intelligent Integrated Management Base. No setup is needed if proxy authentication is not necessary. The information you specify takes effect immediately in the Intelligent Integrated Management Base.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator

API version

v1

Format

Request line

```
POST /application/component/apiVersion/proxyUsers httpVersion
```

Request message body

```
{
    "op": operation,
    "id":user-id,
    "pw": password
}
```

Response message body#

```
{
    "userIdList": [
        "user-id",...
  ]
}
```

#: If `list` is specified for the `op` parameter

Parameters

`op`

Specifies the operation. This parameter cannot be omitted.

- `list`

  Returns the proxy server authentication information configured in the Intelligent Integrated Management Base.

- `add`

  Updates the proxy server authentication information in the Intelligent Integrated Management Base.

- `rm`

Removes the proxy server authentication information configured in the Intelligent Integrated Management Base.

`id`

Specifies the user ID for proxy server authentication. You do not have to specify it if `list` is specified for `op` parameter.

`pw`

Specifies the password for the user ID for proxy server authentication.

You do not have to specify it if `list` or `rm` is specified for `op` parameter.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	None	Processing of the proxy authentication information REST API was successful.
400	KAJY52012-E	The proxy authentication information REST API cannot be executed due to an invalid parameter of the proxy authentication information REST API.
403	KAJY01000-E	There is no permission to run the REST API.
500	KAJY52013-E	The proxy credentials failed to be exclusive.
	KAJY52014-E	The proxy credentials failed to be configured.

Return values

The following information is returned in the response body if the status code is `200`:

The return value varies depending on what is specified for the `op` parameter.

- In `list`

No.	Member name	Data type	Description
1	`userIdList`	array	List of proxy authentication user IDs

- In `add` or `rm`

  None.

  The size of the message body of a response is 0 bytes.

Return values	Description
`2`	Exclusive locked
`3`	Invalid argument
`7`	Request processing is underway
`13`	Update failure error
`255`	System error

Note

This API cannot be executed simultaneously. An error occurs if it is executed.

Examples

The following shows a usage example of the proxy credential setup API.

Request:

```
POST http://hostname:20703/im/api/v1/proxyUsers
{
"op":"list"
}
```

Response:

```
{
  "userIdList": [
    "user001","user002",...
  ]
}
```

5.10 API for linked product

This section describes operations for linked product.

5.10.1 URL information acquisition

Description

Gets the URL to start the monitor window of a linked product that corresponds to the SID of the specified IM management node. Executing this API returns the URL via the `__urlGet` method of the user-created plug-in.

For details on the `__urlGet` method, see *4.4.4(11) __urlGet method*.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/monitorUrl httpVersion
```

Request message body

```
{
    "sid": IM-management-node-SID
}
```

Response message body

```
{
    urlList:[
    {
      "url": URL-for-starting-the-monitor,
      "name": display-name-of-the-URL
    },
    ...
    ]
}
```

Parameters

`sid`

Specifies the SID (management object ID). This parameter cannot be omitted.

Status codes

Status code	Message	Description
200	None	Processing of the URL information acquisition REST API was successful.
400	KAJY02049-E	The URL information acquisition REST API cannot be executed due to an invalid parameter of the URL information acquisition REST API.

Status code	Message	Description
	KAJY22011-E	A nonexistent SID has been specified.
403	KAJY01000-E	There is no permission to run the REST API.
500	KAJY02050-E	An attempt to obtain the URL failed.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`urlList`	object[]	The obtained URL information is returned as an array. If the URL that corresponds to the specified SID does not exist, an array with 0 elements is returned.
2	`url`	string	Specifies the URL for starting the linked product.
3	`name`	string	Specifies the display name of the URL.

Examples

The following shows a usage example of the API to get the URL for starting the monitor of a jobnet (sid:`_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jobgroup/_JP1ROOTJOBNET_jobnet1`) that is a management object.

Request:

```
POST http://hostname:20703/im/api/v1/nodes/monitorUrl
{
"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jobg
roup/_JP1ROOTJOBNET_jobnet1"
}
```

Response:

```
{
  urlList:[
    {
      "url":"http://xxx.xxx.xxx.xxx:22252/ajs/...",
      "name":"JP1/AJS3 - Web Console (List)"
    }
  ]
}
```

5.11 API for trends

This section describes operations for trends.

5.11.1 Metric list acquisition

Description

Gets the list of metrics for time-series data that can be obtained through the SID of the specified IM management node.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/metrics httpVersion
```

Request message body

```
{
    "sid": IM-management-node-SID
}
```

Response message body

```
{
    "metrics": [
      {
        "name": metric,
        "label": metric-display-name,
        "category": category-of-the-metric,
        "description": description-of-the-metric,
        "default": default-setting
      }
      ...
      ]
}
```

Parameters

`sid`

Specifies the SID (management object ID). This parameter cannot be omitted.

Status codes

Status code	Message	Description
200	None	Processing of the metric list acquisition REST API was successful.

Status code	Message	Description
400	KAJY22009-E	The metric list acquisition REST API cannot be executed due to an invalid parameter of the metric list acquisition REST API.
	KAJY22011-E	A nonexistent SID has been specified.
403	KAJY01000-E	There is no permission to run the REST API.
500	KAJY22007-E	An attempt to obtain the list of metrics failed.
	KAJY22008-E	The obtained data is invalid.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`metrics`	object[]	The list of obtained metrics is returned as an array.
2	`name`	string	Is filled with the metric name.
3	`label`	string	Is filled with the display name of the metric. If not specified, it is omitted.
4	`category`	string	Is filled with the category for the metric. If not specified, it is omitted.
5	`description`	string	Is filled with the description of the metric. If not specified, it is omitted.
6	`default`	boolean	Is filled with whether it is the default metric name. • `true`: Default metric • `false`: Non-default metric

Examples

The following shows a usage example of the API to get the list of metrics for a service (sid: `_JP1PFM-M_HOST2/_JP1PFM-AHOST_HOST20/_HOST_HOST20/_JP1PFM-A_serviceID`) of a PFM agent that is a management object.

Request:

```
POST http://hostname:20703/im/api/v1/nodes/metrics
{
"sid":"_JP1PFM-M_HOST2/_JP1PFM-AHOST_HOST20/_HOST_HOST20/_JP1PFM-A_serv
iceID"
}
```

Response:

```
{
    "metrics": [
         {
               "name":"cpu_used_rate",
               "label":"CPU usage",
               "description":"Processer usage (%). Percentage of the el
apsed time where the processor used a thread that is not idle. (Units:
%)",
               "default":true
    } ...
  ]
}
```

5.11.2 Time-series data acquisition

Description

Gets time-series data that corresponds to the SID and metric of the specified IM management node.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/nodes/timeSeries httpVersion
```

Request message body

```
{
    "sid": IM-management-node-SID
    "metric": metric-name,
    "startTime": start-time,
    "endTime": end-time,
    "countPerInstance":upper-limit-for-the-number-of-data-sets-per-inst
ance,
    "instanceCount":upper-limit-for-the-number-of-instances,
}
```

Response message body

```
{
    "metric": "metric",
    "timeSeriesData":[
        {
            "instance": "instance-name",
            "unit":"unit",
            "data":[
                {"time":"time","value": value},
                                 ...
          ]
      },
      ...
    ] ,
    "exceedCountDetected": {
        "countPerInstance": whether-an-excess-of-the-upper-limit-for-th
e-number-of-data-sets-per-instance-is-detected,
        "instanceCount": whether-an-excess-of-the-upper-limit-for-the-n
umber-of-instances-is-detected
    },
    "messageId": "message-id",
    "message": "message"
}
```

Parameters

`sid`

Specifies the SID (management object ID). This parameter cannot be omitted.

`metric`

Specifies the metric to be obtained. This parameter cannot be omitted.

Specify it with half-width alphanumeric characters and the following symbols from 1 to 255 characters:

- (hyphen), _ (underscore)

`startTime`

Specifies the start time of time-series data as the UTC time in ISO8601 format. This parameter cannot be omitted. The number of seconds after the decimal point cannot be specified.

`endTime`

Specifies the endtime of time-series data as the UTC time in ISO8601 format. This parameter cannot be omitted. The number of seconds after the decimal point cannot be specified.

`countPerInstance`

Specifies the upper limit for the number of data sets per instance to be obtained. The range is from 1 to 30,000. Specify it so that the value obtained by multiplying `countPerInstance` paramater by `instanceCount` paramater is less than or equal to 30,000. Omitting this parameter causes the parameter to be set to `60`.

`instanceCount`

Specifies the upper limit for the number of instances to be obtained. The range is from 1 to 30,000. Specify it so that the value obtained by multiplying `countPerInstance` paramater by `instanceCount` paramater is less than or equal to 30,000. Omitting this parameter causes the parameter to be set to `10`.

Status codes

Status code	Message	Description
`200`	None	Processing of the time-series data acquisition REST API was successful.
	KAJY22012-W	Data that is not returned exists because the upper limit value is exceeded.
`400`	KAJY22010-E	The time-series data acquisition REST API cannot be executed due to an invalid parameter of the time-series data acquisition REST API.
	KAJY22011-E	A nonexistent SID has been specified.
`403`	KAJY01000-E	There is no permission to run the REST API.
`500`	KAJY22006-E	An attempt to obtain time-series data failed.
	KAJY22008-E	The obtained data is invalid.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`timeSeriesData`	object[]	The obtained time-series data is returned as an array.
2	`metric`	string	Is filled with the metric name.
3	`instance`	string	Is filled with the instance name. If not specified, it is omitted.
4	`unit`	string	Is filled with the unit of the metric.
5	`data`	object[]	The time and value data is returned as an array.

No.	Member name	Data type	Description
6	`time`	string	The time of time-series data is specified as the UTC time in ISO8601 format. The number of seconds after the decimal point is not specified.
7	`value`	number	The data value is specified.
8	`exceedCountDetected`	object	Whether to detect an excess of the upper limit of the specified parameter value. It has a member for each parameter.
9	`countPerInstance`	boolean	Whether to detect an excess of the upper limit for the number of data sets per instance: • true: Exceeded • false: Not exceeded
10	`instanceCount`	boolean	Whether the number of instances exceeds the upper limit. • true: Exceeded • false: Not exceeded
11	`messageId`	string	The message ID. This is returned only if there is a message to be notified.
12	`message`	string	The message body. The used language is determined by the value specified for the `Accept-Language` property in the HTTP request header. This is returned only if there is a message to be notified.

Examples

The following shows a usage example of the API to get time-series data of a service (sid: `_JP1PFM-M_HOST2/_JP1PFM-AHOST_HOST20/_HOST_HOST20/_JP1PFM-A_serviceID`) of a PFM agent that is a management object.

Request:

```
POST http://hostname:20703/im/api/v1/nodes/timeSeries
{
    "sid":"_JP1PFM-M_HOST2/_JP1PFM-AHOST_HOST20/_HOST_HOST20/_JP1PFM-A_
serviceID",
    "metric":"cpu_used_rate",
    "startTime":"2019-05-22T00:00:00Z",
    "endTime":"2019-05-22T01:00:00Z",
    "countPerInstance":60,
    "instanceCount":10
}
```

Response:

```
{
    "metric":"cpu_used_rate",
    "timeSeriesData":[
            {
                 "unit":"%",
                 "data":[
                  {"time":"2019-05-22T00:00:00Z","value":14.04},
                                ...
               ]
           }
    ],
    "exceedCountDetected": {
        "countPerInstance": true,
        "instanceCount": false
    }
}
```

5.11.3 Write Trend Data

Description

Write trend data to the trend data management DB.

Specify the data to be written in JSON format.

Execution permissions

None

API version

v1

Format

Request line

```
POST /im/api/v1/trendData/write HTTP/1.1
```

Request header

Header name	Setting value
Authorization	Do not set it.

If message body of the request is in JSON format, the other request headers are the same as Common spec of API. For the request header of Common spec of API, see the explanation of the request header in *5.2.3 Request format*.

Request message body

You can send it in the JSON format shown below.

```
{
    "labels":{"__name__": "metric name", "label name": "label value", .
..},
    "samples":[
        [time, value],
        ...
    ]
}
{
    "labels":{"__name__": "metric name", "label name": "label value", .
..},
    "samples":[
        [time, value],
        ...
    ]
}
...
```

Response message body

None

Parameters

Here are the parameters that you specify for message body of the request:

No.	Parameters	Data type	Description
1	labels	Array	Specify the labels for the time series data in an array.
2	__name__	string	Specify a metric name for the time series data. Specification is mandatory.
3	Label Name	string	Specify a label name for the time series data.
4	Label Value	string	Specify label values for temporal data
5	samples	Array	Specify the time series data as an array.
6	Time	Number	Specifies the time of the performance data (the number of milliseconds elapsed since January 1, 1970 00:00:00 (UNIX epoch) in UTC time). You cannot specify a time (negative value) before 0:00:00 a.m. on January 1, 1970.
7	Value	Number	Specify values for the performance data.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API processing succeeded.
500	KAJY62001-E	The Trend Data Management Service returned an error.
	KAJY62000-E	Communication with the Trend Data Management Service failed.
	KAJY62004-E	Failed to get port number for Trend Data Management Service.

Examples

The following is an example of using this API using the OSS curl command.

```
>curl -i --header "Content-Type: application/json" --request POST --data
@c:\\work\\trenddata.json "http://localhost:20703/im/api/v1/trendData/writ
e"
```

trenddata.json

```
{
    "labels":{"__name__":"foo","job":"hoge"},
    "samples":[
        [1617436800000,100]
    ]
}
```

Example of response:

```
HTTP/1.1 200
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Content-Length: 0
Date: Fri, 25 Feb 2022 05:59:58 GMT
```

5.12 API for information management

This section describes operations for information management.

5.12.1 Version information acquisition

Description

Gets the JP1/IM product version and supported REST API versions. This API can be invoked without authentication because it is invoked before all the REST APIs including the login API are invoked.

Execution permissions

None.

API version

None.

Formats

Request line

```
GET /application/component/version httpVersion
```

Request header

The common request header.

Note that you do not specify cookies in the request header.

Request message body

None.

Response header

The common response header.

Response message body

```
{
    "productName": "product-name",
    "productVersion": "product-version",
    "apiVersion": ["REST-API-version", "REST-API-version", ...]
}
```

Parameters

None.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
`200`	--	The version information was retrieved successfully.

Return values

The following information is returned in the response body if the status code is `200`:

No.	Member name	Data type	Description
1	`productName`	string	Returns the name of the product whose version information was retrieved.

No.	Member name	Data type	Description
2	`productVersion`	string	Returns the version of the product in *VV*-*RR* or *VV*-*RR*-*SS* format. For example, the returned value is `12-00` which omits *SS* when the version of the product is 12-00, and the returned value is `12-00-02` when the version of the product is 12-00-02.
3	`apiVersion`	array	Returns an array of the supported REST API versions in *VV*.*RR*.*SS* format. *VV*, *RR*, and *SS* are two-digit numbers. For *apiVersion* in the URI of the REST API request, an array is returned where the value of *VV* is concatenated with a letter `v` with the first digit `0` removed. For example, if the value of *VV* is `01`, *apiVersion* in the URI is `v1`.

Examples

Request:

```
GET /im/api/version HTTP/1.1
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, max-age=0
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: application/json

{
    "productName": "JP1/Integrated Management 3 - Manager",
    "productVersion": "12-00",
    "apiVersion": ["01.00.00"]
}
```

5.13 Suggestion API

This section describes suggestion API-related operations.

5.13.1 Previous execution history acquisition

Description

Gets history information that shows when the response actions corresponding to either the specified IM management node or suggestion IDs were previously executed.

Execution permissions

- `JP1_Console_Admin`
- `JP1_Console_Operator`
- `JP1_Console_User`

API version

v1

Format

Request line

```
POST /application/component/apivVersion/nodes/suggestions/history httpVersion
```

Request message body

```
{
    "sid": tree-SID-of-IM-management-node,
    "suggestionIds": list-of-suggestion-IDs
}
```

Response message body

```
{
    "histories":[
        {
           "suggestionId": suggestion-ID,
           "label": display-name-of-suggestion,
           "jp1UserName": name-of-JP1-user-executing-response-action,
           "startTime": date-and-time-when-response-action-started,
           "endTime": date-and-time-when-response-action-ended,
           "status" : response-action-execution-status
        },
        ...
    ]
}
```

Parameters

`sid`

Specify the tree SID of the IM management node. This parameter cannot be omitted.

`suggestionIds`

Specify a list of suggestion IDs. You can specify a list of 1 to 1,000 suggestion IDs. If you specify an empty list, the error message `KAJY22019-E` is output, and the acquisition of the history of the previously executed response actions stops.

When this parameter is omitted, the history of previously executed response actions is acquired for only those suggestion definitions mapped to the specified IM management node that the logged-in user is qualified to view.

When the specified suggestion IDs correspond to either those suggestions definitions that are not mapped to the tree SID of the specified IM management node or those which the logged-in user is not allowed to view, the error message `KAJY22021-E` is output, and the acquisition of the history of the previously executed response actions stops.

Status codes

The following table describes the status codes that may be returned as a response to the request:

Status code	Message	Description
`200`	None	Successfully acquired the previous execution history.
`400`	`KAJY22019-E`	The request of the REST API is invalid. The possible causes are: invalid format of the tree SID of the IM management node, invalid suggestion IDs, invalid number of lists of suggestion IDs, etc.
	`KAJY22022-E`	The request of the REST API is invalid. There are duplicate suggestion IDs.
	`KAJY22011-E`	Either the specified tree SID does not exist or the logged-in user does not have the permission to view the specified IM management node.
	`KAJY22021-E`	The specified suggestion IDs correspond to either those suggestions that are not mapped to the specified IM management node or those which the logged-in user is not allowed to view.
`403`	`KAJY01000-E`	The logged-in user does not have the permission to execute the REST API.

When the status code is `200`, the following information is returned in the response body:

No.	Member name	Data type	Description
1	`histories`	object[]	Returns the history of previously executed response actions as an array. When there are no suggestion definitions that are mapped to the tree SID of the specified IM management node, or when the logged-in user is allowed to view none of the suggestion definitions mapped to the tree SID of the specified IM management node, an empty array is returned.
2	`suggestionId`	string	Sets the suggestion ID.
3	`label`	string	Sets the display name of the suggestion.
4	`jp1UserName`	string	The name of the JP1 user executing the response action. This member is not returned when there is no previous execution history.
5	`startTime`	string	Returns the date and time when the response action was executed, as UTC time in ISO 8601 format. This member is not returned when there is no previous execution history.
6	`endTime`	string	Returns the date and time when the execution of the response action was completed, as UTC time in ISO 8601 format. When the response action is currently being executed or has failed, an empty string is returned. This member is not returned when there is no previous execution history.

No.	Member name	Data type	Description
7	`status`	int	The execution status of the response action. One of the following values is returned: • `0`: Currently being executed • `1`: Successfully executed • `2`: Failed This member is not returned when there is no previous execution history.

Examples

The following example shows how to use this API:

Request:

```
POST http://hostname:20703/im/api/v1/nodes/suggestions/history
{
    "sid":"_ROOT_AllSystems/_HOST_HOSTA/_CATEGORY_managementApplication
s/_OBJECT_JP1IMMGR"
}
```

Response:

```
{
    "histories":[
        {
            "suggestionId":"exec_jim_log",
            "label":"Execution of JP1/IM data collection tool",
            "jp1UserName":"jp1admin",
            "startTime":"2020-03-01T00:00:00Z",
            "endTime":"",
            "status" :0
        },
        {
            "suggestionId":"reg_ticket",
            "label":"Registration of ticket to Redmine",
            "jp1UserName":"jp1admin",
            "startTime":"2020-03-01T00:00:00Z",
            "endTime":"2020-03-01T00:00:10Z",
            "status" :1
        }
    ]
}
```

5.13.2 Response action suggestion

Description

Compares the suggestion definitions against the suggestion activation criteria and suggests response actions appropriate to the system status, according to the specified IM management node or suggestion ID.

Execution permissions

- `JP1_Console_Admin`
- `JP1_Console_Operator`
- `JP1_Console_User`

API version

v1

Format

Request line

```
POST /application/component/apivVersion/nodes/suggestions/suggest httpV
ersion
```

Request message body

```
{
    "sid": tree-SID-of-IM-management-node,
    "suggestionIds": list-of-suggestion-IDs
}
```

Response message body

```
{
    "suggestions":[
        {
            "suggestionId": suggestion-ID,
            "label": display-name-of-suggestion,
            "status": whether-suggestion-activation-criteria-are-satisf
ied,
            "cases":[
                [
                    {
                        "description": description-of-criterion,
                        "status": status-of-criterion,
                        "acquisitionDate": acquisition-date-and-time,
                    },
                    ...
                ],
                [
                    {
                        "description": description-of-criterion,
                        "status": status-of-criterion,
                        "acquisitionDate": acquisition-date-and-time,
                    },
                ...
            ],
            "action": {
                    "type": type-of-response-action,
                    "params": parameters-of-response-action,
                    "description": description-of-response-action
                      }
            "messageList":[
                {
                    "messageId": message-ID,
                    "message": message-text
                },
                ...
            ]
        },
        ...
    ]
}
```

Parameters

`sid`

Specify the tree SID of an IM management node.

`suggestionIds`

Specify a list of suggestion IDs. You can specify a list of 1 to 1,000 suggestion IDs. If you specify an empty list, the error message `KAJY22019-E` is output, and the response action suggestion processing stops.

When this parameter is omitted, only those suggestion definitions mapped to the specified IM management node that the logged-in user is allowed to view are compared against the suggestion activation criteria to judge if they satisfy the criteria, and information regarding the suggested response actions that are appropriate to the system status is subsequently acquired.

When the specified suggestion IDs correspond to either those suggestions definitions that are not mapped to the tree SID of the specified IM management node or those which the logged-in user is not allowed to view, the error message `KAJY22021-E` is output, and the acquisition of response action suggestion information stops.

Status codes

The following table describes the status codes that may be returned as a response to the request:

Status code	Message	Description
`200`	None	Response actions were successfully suggested.
	`KAJY22026-W`	Failed to convert the variables in the suggestion definitions.
	`KAJY22027-W`	Suggestion information obtained by the conversion of variables in the suggestion definitions is invalid.
	`KAJY22028-W`	Failed to make a judgment as to whether the suggestion activation criteria are satisfied.
	`KAJY22047-W`	Failed to acquire information from the Repeated event list window.
`400`	`KAJY22020-E`	The request of the REST API is invalid. The possible causes are: invalid format of the tree SID of the IM management node, invalid suggestion IDs, invalid number of lists of suggestion IDs, etc.
	`KAJY22022-E`	The request of the REST API is invalid. There are duplicate suggestion IDs.
	`KAJY22011-E`	Either the specified tree SID does not exist or the logged-in user does not have the permission to view the specified IM management node.
	`KAJY22021-E`	The specified suggestion IDs correspond to either those suggestions that are not mapped to the specified IM management node or those which the logged-in user is not allowed to view.
`403`	`KAJY01000-E`	The logged-in user does not have the permission to execute the REST API.

When the status code is `200`, the following information is returned in the response body:

No.	Member name		Data type	Description
1	`suggestions`		object[]	Returns the acquired suggestion information as an array. When there are no suggestion definitions that are mapped to the tree SID of the specified IM management node, or when the logged-in user is allowed to view none of the suggestion definitions mapped to the tree SID of the specified IM management node, an empty array is returned.
2		`suggestionId`	string	Sets the suggestion ID.
3		`label`	string	Sets the display name of the suggestion.
4		`status`	int	Indicates whether the suggestion activation criterion was satisfied. One of the following values are returned:

No.	Member name	Data type	Description
			- 0: Criterion satisfied - 1: Criterion not satisfied - 2: Error
5	cases	object[][]	Returns double-array data of suggestion criteria objects. The inner array represents a group of AND conditions whereas the outer array represents a group of OR conditions. This member is not returned when the cases member is not specified in the suggestion definitions.
6	description	string	Returns the description of the criterion after conversion of the variables.
7	status	int	The status of a criterion. One of the following values is returned: - 0: Not judged - 1: Match - 2: Does not match - 3: Error
8	acquisitionDate	string	Returns the date and time when criterion information was acquired, as UTC time in ISO 8601 format. When status (status of criterion) is 0 (Not judged) or 3 (Error), an empty string is returned.
9	action	object	Information regarding a response action is returned.
10	type	string	The type of response action specified in the suggestion definition is returned. For details on the type member, see *(2) Response action* in *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.
11	params	object	When jump is specified as type of the response action and at the same time relatedEvent is also specified, relatedEvent and members no. 12 to 15 are returned. In all the other cases, the parameters of the response action specified in the suggestion definition are returned with their variables converted. For details on the members other than members no. 12 to 15, see *(2) Response action* in *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.
12	suppressId	int	The value of the E.JP1_IMSUPPRESS_ID attribute (suppressed event ID) of the JP1 event specified with relatedEvent#
13	eventSevere	int	The value of the E.@JP1IM_SEVERE attribute (severe event) of the JP1 event specified with relatedEvent#
14	suppressName	string	The value of the E.JP1_IMSUPPRESS_NAME attribute (repeated event condition name) of the JP1 event specified with relatedEvent#
15	nodeSid	string	The tree SID of the IM management node to which the JP1 event specified with relatedEvent# belongs
16	description	string	- When status (whether the suggestion activation criterion was satisfied) is 0 (criterion satisfied): Returns the description of response action with the variables converted. - When status is other than 0: Returns the description of response action without the variables being converted. If the returned string exceeds 512 characters, it is truncated to 512 characters.
17	messageList	object[]	Returns the warning message issued during processing that does not prevent the processing from continuing.

No.	Member name	Data type	Description
			This member is not returned when there is no warning message that does not prevent the processing from continuing.
18	messageId	string	Returns a message ID.
19	message	string	Returns message text.

#

For details on `relatedEvent`, see information regarding `relatedEvent` provided in *(2)(A)(e) Response action when type is set to jump* in *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.

Examples

The following example shows how response actions are suggested for the IM management node (tree SID: `_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows/_OBJECT_JP1PFM-ATA1HOST2`) that belongs to the service provided by the PFM agent that constitutes a management object.

Request:

```
POST http://hostname:20703/im/api/v1/nodes/suggestions/suggest
{
"sid":"_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1
%2FPFM%20-%20Windows/_OBJECT_JP1PFM-ATA1HOST2"
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "suggestions":[
        {
            "suggestionId":"check_affected_rootJobnet",
            "label":"Impact on root jobnets affected by host going down
",
            "status":0,
            "cases":[
                [
                    {
                         "description":"A JP1/AJS - Agent node exists o
n the same host where the selected node (PFM - Agent) exists",
                         "status":1,
                         "acquisitionDate":"2020-03-11T11:00:00Z"
                    },
                    {
                         "description":"A JP1 event indicating that th
e host stopped has been issued",
                        "status":1,
                         "acquisitionDate":"2020-03-11T11:00:01Z"
                    },
                    {
                         "description":"The host of the selected node i
s down",
                         "status":1,
                         "acquisitionDate":"2020-03-11T11:00:02Z"
                    }
                ]
            ],
            "action":
                {
                    "type":"jump",
                    "params":
                        {
                            " url":"index?sid=%5FROOT%5FAllSystems%2F%5
FHOST%5FHOST1%2F%5FCATEGORY%5FmanagementApplications%2F%5FOBJECT%5FJP1A
JSAGT&view=tree&tab=relation&eou=1"
                        },
                    "description":"Move to the Related node tab display
ing the JP1/AJS - Agent node"
                }
        }
    ]
}
```

5.13.3 Response action execution

Description

Executes the specified response action.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator
- JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apivVersion/nodes/suggestions/action httpVe
rsion
```

Request message body

```
{
    "sid": tree-SID,
    "suggestionId": suggestion-ID,
    "action": {
             "type": type-of-response-action,
             "params": parameters-of-response-action,
             "description": description-of-response-action
              }
}
```

Response message body

```
{
    "location": URL-of-destination-screen,
    "target": target-attribute-of-html-for-opening-URL-of-destination-s
creen,
    "suppressId":information-provided-in-the-Repeated-event-list-window
-(suppressed-event-ID),
    "eventSevere":information-provided-in-the-Repeated-event-list-windo
w-(severe-event),
    "suppressName":information-provided-in-the-Repeated-event-list-wind
ow-(repeated-event-condition-name),
    "nodeSid":information-provided-in-the-Repeated-event-list-window-(t
ree-SID-of-IM-management-node),
    "message":{
        "messageId": message-ID,
        "message": message-text
    }
}
```

Parameters

`sid`

Specify a tree SID.

`suggestionId`

Specify a suggestion ID. For details on the suggestion ID, see information regarding `suggestionId` in *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.

`action`

Specify a response action.

- `type`: Specify the type of response action. For details on the specifiable types of response actions, see *(2) Response action* in *Suggestion definition file (imdd_suggestion.conf)* in *Chapter 2. Definition Files*.
- `params`: Specify the response action's parameters after conversion of the variables. When the type of response action is `jump` and at the same time `relatedEvent` is also specified, the following members must also be specified. For details on each of these members, see *5.13.2 Response action suggestion*.

  - `suppressId`

  - `eventSevere`

  - `suppressName`

  - `nodeSid`
- `description`: Specify the description of the response action after conversion of the variables. You can specify a string not exceeding 512 characters, which must not include control characters. The specification of an empty string is not allowed.

Status codes

The following table describes the status codes that may be returned as a response to a request:

Status code	Message	Description
`200`	None	The response action execution REST API was successfully processed.
	`KAJY22029-W`	The response action is currently being executed.
`400`	`KAJY22031-E`	The request of the REST API is invalid. The possible causes are: invalid format of the tree SID of the IM management node, invalid suggestion IDs, invalid response action, etc.
	`KAJY22011-E`	Either the specified tree SID does not exist or the logged-in user does not have the permission to view the specified IM management node.

Status code	Message	Description
	KAJY22021-E	The specified suggestion IDs correspond to either those suggestions that are not mapped to the specified IM management node or those which the logged-in user is not allowed to view.
403	KAJY01000-E	The logged-in user does not have the permission to execute the REST API.
500	KAJY22033-E	The upper limit of concurrent executions for the response action is exceeded.

When the status code is 200, the following information is returned in the response body:

No.	Member name	Data type	Description
1	location	string	Returns the URL of the destination screen. • When the type of response action is jump and at the same time url is also specified: Returns the URL of the screen to which to jump. • In all the other cases: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
2	target	string	Returns the target attribute of HTML used for opening the URL of the destination screen. • When the type of response action is jump and at the same time url is also specified: Returns the target attribute of the HTML used for opening the URL of the screen to which to jump. • When the type of response action is other than jump: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
3	suppressId	string	Returns the information (suppressed event ID) provided in the Repeated event list window. • When the type of response action is jump and at the same time url is also specified: Returns the information (suppressed event ID) provided in the Repeated event list window. • In all the other cases: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
4	eventSevere	string	Returns the information (severe event) provided in the Repeated event list window. • When the type of response action is jump and at the same time relatedEvent is also specified: Returns the information (severe event) provided in the Repeated event list window. • In all the other cases: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
5	suppressName	string	Returns the information (repeated event condition name) provided in the Repeated event list window. • When the type of response action is jump and at the same time relatedEvent is also specified:

No.	Member name		Data type	Description
				Returns the information (repeated event condition name) provided in the Repeated event list window. - In all the other cases: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
6	`nodeSid`		string	Returns the information (tree SID of the IM management node) provided in the Repeated event list window. - When the type of response action is `jump` and at the same time `relatedEvent` is also specified: Returns the information (tree SID of the IM management node) provided in the Repeated event list window. - In all the other cases: This member is not returned. When the response action is being executed, this member is not returned regardless of the type of response action.
7	`message`		object	When the response action is being executed, a message notifying the user that the response action is being executed is returned. When the response action is not being executed, this member is not returned.
8		`messageId`	string	Returns the message ID.
9		`message`	string	Returns the message text.

Notes

The maximum number of concurrent executions of this API is 10. When the maximum limit is exceeded, the error message `KAJY22033-E` is output, and the execution of the response action stops.

Examples

The following example shows how to execute the response action (suggestion ID: `check_affected_rootJobnet`) that consists of *Move to the Related node tab displaying the JP1/AJS-Agent node* for the IM management node (tree SID: `_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows/_OBJECT_JP1PFM-ATA1HOST2`) that belongs to the service provided by the PFM agent that constitutes a management object.

Request:

```
POST http://hostname:20703/im/api/v1/nodes/suggestions/action
{
    "sid":"_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY
_JP1%2FPFPM%20-%20Windows/_OBJECT_JP1PFM-ATA1HOST2",
    "suggestionId":"check_affected_rootJobnet",
    "action":
        {
            "type":" jump",
            "params":
                {
                    "url":"index?sid=%5FROOT%5FAllSystems%2F%5FHOST%5FH
OST1%2F%5FCATEGORY%5FmanagementApplications%2F%5FOBJECT%5FJP1AJSAGT&vie
w=tree&tab=relation&eou=1"

                },
            "description":"Move to the Related node tab displaying the
JP1/AJS - Agent node"
```

```
        }
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "location":"index?sid=%5FROOT%5FAllSystems%2F%5FHOST%5FHOST1%2F%5FC
ATEGORY%5FmanagementApplications%2F%5FOBJECT%5FJP1AJSAGT&view=tree&tab=
relation&eou=1",
    "target":""
}
```

5.14 OpenID authentication API

This section describes the operations related to the OpenID authentication API.

5.14.1 Single sign-on mapping definition application

Description

Applies the mapping information defined in the single sign-on mapping definition file (`imdd_sso_mapping.properties`) to the Intelligent Integrated Management Base. The set information is immediately applied to the Intelligent Integrated Management Base.

If the definition is applied when the single sign-on mapping definition file has no valid property at all, the `KAJY52031-W` message is added to the response and the applied single sign-on mapping definitions are cleared.

For details on the single sign-on mapping definition file (`imdd_sso_mapping.properties`), see *Single sign-on mapping definition file (imdd_sso_mapping.properties)* in *Chapter 2. Definition Files*.

Execution permissions

- `JP1_Console_Admin`
- `JP1_Console_Operator`

API version

v1

Format

Request line

```
POST /application/component/apivVersion/updateSsoMap httpVersion
```

Request message body

None

Parameters

None

Status codes

The following table describes the status codes that may be returned as a response to a request:

Status code	Return value	Message	Description
200 403	--	None	The single sign-on mapping definition application REST API was successfully processed.
		KAJY52031-W	The single sign-on mapping definition file has no valid definition.
500	7	KAJY01000-E	The logged-in user does not have the permission to execute the REST API.
500	2	KAJY52022-E	Failed to establish exclusive control for single sign-on mapping definitions.
	13	KAJY52023-E	Failed to apply the single sign-on mapping definition.
	14	KAJY52026-E	The single sign-on mapping definition file was not correctly loaded.

Return values

The following table describes the return values:

Return value	Description
2	Failed to establish exclusive control
7	Execution permission error
13	Update error
14	Definition file load error
255	System error

Notes

- Concurrent executions of this API are not allowed. Concurrent executions of this API result in an error.
- When an error occurs during the execution of this API, an error message is output to the integrated trace log. An API error response containing the error message is returned to the caller of the API. Using the information provided in the received response, the caller displays the message. When the REST API is called from the `jddupdatessomap` command and an error response is subsequently returned, error information is output to the standard error output. For details on the `jddupdatessomap` command, see *jddupdatessomap* in *Chapter 1. Commands*.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/updateSsoMap HTTP/1.1
Authorization: Bearer xxxx
Accept-Language: ja
Content-Type: application/json
Accept: application/json
```

Response at the end of the warning:

```
  {
  "messageList": [
    {
      "messageId": "KAJY52031-W",
      "message": "The Single Sign-on mapping definition file does not c
ontain a valid definition."
    }
  ]
}
```

5.15 Distribution API

This section describes distribution API-related operations.

5.15.1 Get distribution (File download)

Description

Download the distribution (file) specified in the request line.

Execution permissions

None#

#

You must have execute permissions for the Login API used to log in to the Intelligent Integrated Management Base.

API version

None

Format

Request line

```
GET /download/Distribution directory name/distribution file name HTTP/1
.1
```

Request header

Header name	Setting value
Accept	Do not specify it. Even if specified, "`application/zip`" is assumed if the file to be downloaded is in zip format, and "`application/x-gzip`" is assumed if the file to be downloaded is in gz format.

If message body of the request is in JSON format, the other request headers are the same as Common spec of API. For the request header of Common spec of API, see the explanation of the request header in *5.2.3 Request format*.

Request message body

None

Response message body

Contents of the distribution's files

Parameters

Here are the parameters that you specify for message body of the request:

No.	Parameters	Data type	Description
1	Distribution directory name	string	Specify the distribution directory as required. If you specify a directory name for a distribution that does not exist, the distribution retrieval fails.
2	Distribution file name	string	Specify the distribution directory as required. If you specify a file name for a distribution that does not exist, the distribution retrieval fails.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	OK	API processing succeeded.
403	Forbidden	Not authenticated,Authentication information is incorrect.
404	Not Found	The specified distribution does not exist, and in a Windows environment, the distribution cannot be accessed. However, in the case of a Windows environment, if you do not have access authority to the distributed file itself, no error will occur, and communication will be closed after a few minutes of non-response.

If the status code is 200, the contents of the distribution file are returned to the message body of the response.

Notes

JP1/IM - The following are the requirements for distributions (files) to be stored in Manager (Linux).

■Distribution files

- Can be handled as a file
- he file must be compressed (gz format if the distribution destination is Linux environment, zip format if the distribution destination is Windows environment)
- The file name should follow the "zueng031.tifNaming convention for distribution file name and storage destination directory name" below.
- Grant the following permissions to the file:

Permissions	Owner	Group
`-r--r--r--`	`root`	`root`

- The maximum file size is 300MB.

■Directory to create to store distributions

- Create a directory to store the same distribution in the following storage location, and store the distribution in the created directory.

Storage location
`/opt/jp1imm/public/download`

- The directory name should follow the "■Naming convention for distribution file name and storage destination directory name" shown below.
- Grant the following permissions to the directory:

Permissions	Owner	Group
`drwxr-xr-x`	`root`	`root`

■Naming convention for distribution file name and storage destination directory name

[Reserved words]

File and directory names that begin with the following strings are reserved words: It is not case sensitive.

- `hitachi_`
- `jp1_`

The above reserved words are used when distributing files within the scope of functions and services provided by Hitachi products or JP1 products (including JP1/IM - Agent). It cannot be used to distribute other user-specific files.

[Allowed characters]

The following characters are allowed in file and directory names:

- Alphanumeric characters
- `-` (hyphen)
- `.` (period)
- `_` (underscore)

■Distribution's file path, including extension

- Must be 235 characters or less

  If an environment variable is used for the file path, the file path (including extension) of the distribution after the environment variable is expanded must be 235 characters or less.

■Providers of Distributed Products

- The provider of the distribution (distributed product) shall provide a way to check the version information of the distribution.

  You can check the version information of the JP1/IM - Agent in the version file (Version.txt).

  For details on where to store version file of JP1/IM - Agent, see *(3) Integrated agent host (Windows)* and *(4) Integrated agent host (Linux)* in *Appendix A.4 JP1/IM - Agent* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

Examples

Example of request:

```
GET http://hostname:20703/download/im2-agent/xxx.zip
```

5.16 API for Execute for Auto/Manual Response Action

This section describes API for Execute for Auto/Manual Response Action-related operations.

5.16.1 Obtain execution result of Response Action

Description

Gets the execution result of Response Action.

If you set the search criteria to a parameter, you retrieve the execution result of Response Action that match the search criteria.

Execution permissions

Following permissions are required:

When only one key "execDetailEventSid" is specified in the filter:

- JP1 permission level: JP1_Console_Admin, JP1_Console_Operator, JP1_Console_User

In other cases:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin, JP1_Console_Operator, JP1_Console_User

API version

v1

Format

Request line

```
POST /application/component/apiVersion/responseActions/results httpVers
ion
```

Request message body

```
{
  "type":"Process content",
  "direction":"ResponseAction execution result acquisition direction",
  "searchType":Search type,
  "count":Acquired number of ResponseAction execution results,
  "since":"Search start position action SID",
  "lastDirection":"Search direction for response action results specifi
ed in the previous search process"
  "dbInfo":[
          {
             "beginData":"Search start position action SID",
             "endData":"Search end position action SID",
             "since":"Action SID for the search start position specifie
d in the previous search process"
          }
        ]
  "filter":[    //ResponseAction result search filters
    {"key":"Search key","ope":"Compare keyword","val":["operand 1",...]
},
    ...
  ]
}
```

Response message body

```
{
  "actionResult":[  //ResponseAction result
    {
      "actionSid":"ResponseAction SID",
      "executionHost":"Destination host Name",
      "actionName":"Action name",
      "executionCommand":"Command",
      "actionStatus":"Action status",
      "targetSid":"Execute target SID",
      "executionDeal":"Execute trigger",
      "executionDetailInfo":"Execute trigger detailed Information",
      "actionType":"Action type",
      "actionAcceptTime":"ResponseAction reception time",
      "actionSendTime":"ResponseAction input time",
      "actionEndTime":"ResponseAction end time",
      "executionResult":["Execute result"],
      "returnValue":"Return value",
      "message":["Message"]
    },
    ...
  ],
  "beginData":"ResponseAction execution result search start position Re
sponseAction result information",
  "endData":"ResponseAction result information of the search end positi
on of the ResponseAction execution result",
  "dbInfo":"Next search information for the execution result of Respons
eAction for distribution DB",
  "messageList":[
    {
      "messageId":"Message ID",
      "message":"Message"
    },
    ...
  ]
}
```

Parameters

Here are the parameters that you specify for message body of the request:

Member name	Data type	Optional	Description
`type`	string	No	Specifies the execution result of the ResponseAction to retrieve. • list Get a list of ResponseAction findings • detail Get ResponseAction result detail info If a value other than the above is specified, error is returned.
`direction`	string	Yes	Specify the search direction for ResponseAction execution results. • past Search in the past direction • future Search for future directions The default is "past". If a value other than the above is specified, Error is returned.

Member name	Data type	Optional	Description
`searchType`	int	No	Specify the search type. • `0`: Action SID specification Specify the target SID for `since` and `1` for `count`. • `1`: Latest page • `2`: New page • `3`: Update • `4`: Old page • `5`: Oldest page If you specify anything other than the above, an error will occur.
`count`	int	Yes	Specify a range from 1 to 2,000 for the maximum number of results of ResponseAction execution that can be acquired. The default is 100. If a value other than the above is specified, Error is returned.
`since`	string	Yes	Specify the search start position of the ResponseAction execution result with the corrective action SID. It is specified as a character string of less than 1024 bytes. Otherwise, it is Error. Search for past or future ResponseAction execution results from the specified action SID (The ResponseAction execution result of the specified ResponseAction SID is not included in the search target. However, if count is 1, the specified action SID is searched.) If omitted, the search starts from the beginning or end of the ResponseAction result management database according to the specified direction. For setting method, see ■*About setting method for since and direction for retrieval target* below.
`lastDirection`	string	Yes	Specifies the search direction for response action results specified in the previous search procces. Specify "past" for the past direction and "future" for the future direction. Required if `searchType` is 2 or 4. If you specify anything other than the above, an error will occur.
`dbInfo`	object[]	Yes	ResponseAction is an Execute control for ResponseAction that specifies the starting and ending position for ResponseAction results-management database search. It can be omitted when searching from the beginning (Latest) for the first time. From the next time onwards, specify the content of dbInfo returned in the previous return Value. For setting method, see ■*About setting method for since and direction for retrieval target* below.
`beginData`	string	Yes	Specifies the ResponseAction SID of the search start position for the ResponseAction execution result. It is specified as a character string of less than 1024 bytes. Otherwise, it is Error.
`endData`	string	Yes	Specifies the ResponseAction SID of the search end position for the ResponseAction execution result. It is specified as a character string of less than 1024 bytes. Otherwise, it is Error.
`since`	string	Yes	The action SID of the search start position when the previous search type was 1, 2, 4, 5. Set it to less than 1024 bytes. Otherwise, an error will occur.

Member name	Data type	Optional	Description
`filter`	object[]	Yes	An object that specifies the filter for obtaining the execution result of ResponseAction. For details, see ■*About ResponseAction result search filter* below.

■About setting method for since and direction for retrieval target

Object of acquisition	searchType	since	direction	Additional setting
Latest (First time)	1	Empty character (can be omitted)	past	None
Oldest	5	Empty character (can be omitted)	future	None
Transition to a new page	2	Setup the most recent (last in the array sequence) actionSid from actionResult of the previous search response.	future	dbInfo is mandatory. `lastDirection` is mandatory.
Transitions to one old page	4	Setup the oldest (first in the array sequence) actionSid from actionResult of the previous search response.	past	dbInfo is mandatory. `lastDirection` is mandatory.
Update (Refresh)	3	Setup value that was the same as since of the last search.	Setup value that was the same as direction of the last search.	dbInfo is mandatory. `lastDirection` can be omitted.
Get detailed Information by ResponseAction SID specification	0	Setup ResponseAction SID you want to retrieve.	past/future	Set count to 1 and set "detail" to type. `lastDirection` can be omitted.

Note: If the above configuration file content is invalid, correct results may not be obtained. If so, execute again from Latest page-first retrieval.

■About ResponseAction result search filter

This section explains how to specify parameters.

```
{
"key":"Search key","ope":"Comparison keyword","val":["operand 1","operand
2",...]
}
```

Table 5–14: Combinations of attribute name and compare keywords that can be specified

Search key (Value to setup)	Data type	Comparison keywords	Operand
ResponseAction SID (actionSid)	string	• Full match (MATCH) • Regular expression (REGEX)	Specify ResponseAction SID. You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is Error. If you specify a regular expression, you cannot specify more than one. If more than one value is specified, error is set.
Destination host name (executionHost)	string	• Full match (MATCH) • Regular expression	Specifies host name that execute ResponseAction. You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is error.

Search key (Value to setup)		Data type	Comparison keywords	Operand
			(REGEX)	If you specify a regular expression, you cannot specify more than one. If more than one value is specified, error is returned.
Action status (actionStatus)		string	• Full match (MATCH)	Specifies status of ResponseAction. You can specify more than one. The following values can be specified: • send (Execution destination sending) • queue (Queuing) • running (Execution in progress) • ended (Exit) • unknown (Status unknown) • none (None) • fail (Fail) • senderror (Communication failure) • error (Execution failure) If a value other than the above is specified, error is returned.
Action name (actionName)		string	• Full match (MATCH) • Regular expression (REGEX)	Specifies action name of ResponseAction. You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is error. You can specify any character other than the control character (0x00 to 0x1F,0x7F to 0x9F). If you specify a regular expression, you cannot specify more than one. If more than one value is specified, Error is returned.
Execution trigger detailed information		--	--	Specifies execution trigger for ResponseAction. For auto ResponseAction, for JP1 event SID, manual ResponseAction, specify JP1 user name who requested the manual execution.
	JP1 Events. SID (execDetailEventSid)	string	• Full Match (MATCH)	Specifies SID of JP1 events. You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is error.
	JP1 user name (execDetailUserName)	string	• Full match (MATCH) • Regular expression (REGEX)	Specify JP1 user name. You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is error. If you specify a regular expression, you cannot specify more than one. If more than one value is specified, error is returned.
ResponseAction reception time (actionAcceptTime)		string	• Date/time specification (TRANGE)	Specifies the time when ResponseAction execution control received a ResponseAction execution request. The input format is the extended form of ISO 8601 (YYYY-MM-DDThh:mm:ssTZD), otherwise it is error. Specify the starting date/time, and then the ending date/time. If you do not enter a starting date/time, retrieve all date/time data prior to the ending date/time. If you do not enter an exit date/time, retrieve all of the later date/time from the starting date/time.
Return value (returnValue)		string	• Full match (MATCH)	Execute specifies the return value of the finding.

Search key (Value to setup)	Data type	Comparison keywords	Operand
		• Regular expression (REGEX)	You can specify a maximum of 100 items in the range of 1 to 4096 bytes. Otherwise, it is error. If you specify a regular expression, you cannot specify more than one. If more than one value is specified, Error is returned.

■About regular expressions

The following regular expressions are used in ResponseAction result finding filter:

- For Windows: Extended regular expressions (XPG4 compliant)
- For Linux: Extended Regular Expressions (POSIX1003.2)

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	--
200	KAJY63041-W	Some execution results cannot be obtained because communication with the ResponseAction execution control, which is the destination for obtaining ResponseAction execution results, cannot be established.
200	KAJY63042-W	An error is returned from the ResponseAction execution control at the ResponseAction execution result acquisition destination, and some execution results cannot be obtained.
400	KAJY63302-E	REST API parameter was specified incorrectly. <Cause> • A parameter that cannot be omitted is omitted. • You set a value that cannot be set • Character limit exceeded • The maximum number of items that can be specified is exceeded. • Duplicate search key
400	KAJY63303-E	JSON formatting of the request message body is invalid.
403	KAJY01000-E	You do not have permission to execute REST API.
500	KAJY63040-E	Execute destination cannot be obtained from the system configuration information. (There is no management node for the execution request destination host in the system configuration.)
		Execute destination could not be obtained from the system configuration information. (The integrated agent management base that manages the execution request destination host could not be obtained.)
500	KAJY63039-E	The system configuration information is not accessible.
500	KAJY63333-E	An unexpected error occurred in REST API processing.
500	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).

Return values

- When the status code is 200

  Returns the data shown in the following tables to message body of the response.

  The returned information differs depending on the value specified in the request parameter type.

Member name		Data type	Value of type		Description
			list	detail	
actionResult		object[]	Y	Y	ResponseAction result object. The members returned depend on value specified in type of request parameters.
	actionSid	string	Y	Y	Returns ResponseAction SID.
	executionHost	string	Y	Y	Returns the destination host. • When action type is "cmd" Host name of the execution destination integrated JP1/IM agent control base • When action type is not "cmd" ResponseAction execute control host name
	actionName	string	Y	Y	Returns action name.
	executionCommand	object	Y	Y	Returns the execution command. The object to be returned depends on action type. • When Action type is "cmd" See ■*When action type is "cmd"* table below. • When action type is "restapi" See ■*When action type is "restapi"* table below. • When action type is "eventstatus" See ■*When action type is "eventstatus"* table below.
	actionStatus	string	Y	Y	Returns status of ResponseAction.
	targetSid	string	Y	Y	Returns the configuration SID of the system (JP1/IM agent control base, or JP1/IM - Manager) that execute ResponseAction.
	executionDeal	string	Y	Y	Returns the timing when ResponseAction is executed.
	executionDetailInfo	string	Y	Y	Returns detailed information at the time ResponseAction was executed. • For auto ResponseAction (JP1 event trigger) JP1 Events SID • For manual ResponseAction JP1 user name that made the execution request
	actionType	string	Y	Y	Returns type of ResponseAction to be executed. Value to be returned is shown below. • cmd • restapi • eventstatus
	actionAcceptTime	string	Y	Y	Returns the time when the ResponseAction execution control accepted the ResponseAction execution request.
	actionSendTime	string	Y	Y	Returns the time when the ResponseAction execution control sent the ResponseAction execution request.
	actionEndTime	string	Y	Y	Returns the time when the execution of the ResponseAction is completed.
	executionResult	string[]	N	Y	Returns a execution result. • When action type is "cmd" Command standard output and standard error output

Member name		Data type	Value of type		Description
			list	detail	
					• When action type is "restapi" REST API response body • When action type is "eventstatus" Return object of event handling status change method
	`returnValue`	string	Y	Y	Returns the return value of the execution result. • When action type is "cmd" Command-return value • When action type is "restapi" REST API status code • When action type is "eventstatus" The value is 0 if the event handling status change was successful, and 1 if it failed.
	`message`	string[]	N	Y	This is message output by ResponseAction execution control.
`beginData`		string	Y	Y	Returns the ResponseAction SID next to the search start position of the ResponseAction execution result. Omit if there is no ResponseAction SID after the search start position.
`endData`		string	Y	Y	Returns the ResponseAction SID next to the search end position of the ResponseAction execution result. Omit if there is no ResponseAction SID after the search end position.
`dbInfo`		object[]	Y	Y	This is an object that returns the search start and end positions of the distributed DB response action results.
	`beginData`	string	Y	Y	Returns the ResponseAction SID of the search start position of the ResponseAction execution result. Omit if there is no search target ResponseAction execution result.
	`endData`	string	Y	Y	Returns the ResponseAction SID of the search end position of the ResponseAction execution result. Omit if there is no search target ResponseAction execution result.
	`since`	string	Y	Y	Returns the action SID of the search start position when 1,2,4,5 was specified as the previous search type.
`messageList`		object[]	Y	Y	Only returned if there is a continuable warning message that occurred in processing.
	`messsageId`	string	Y	Y	Returns message ID.
	`message`	string	Y	Y	Returns message.

Legend

Y: The information of the applicable member is returned.

N: The information on the applicable member is not returned

■When action type is "cmd"

Member name	Data type	Description
`cmd`	string	Returns the command name.

Member name	Data type	Description
envFile	string	Returns environment-variable file name and pass.

■When action type is "restapi"

Member name	Data type	Description
method	string	Returns REST API method.
url	string	Returns URL of REST API.
headers	object	Returns REST API request headers.
body	string	Returns REST API request body. Omit the request body if it is not needed.

■When action type is "eventstatus"

Member name	Data type	Description
dealt	string	Returns event status.
eventSid	string	Returns SID of JP1 events.

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an Error occurs is returned. However, "returnCode" items are omitted.

  When a warning has occurred, a warning information similar to the one with status code 200 is added to the item "extensions" (extended information) and returned to the requestor.

Examples

Request:

The following is an example of how to use the API to set search conditions as parameters and acquire information in the ResponseAction result list.

```
POST http://hostname:20703/im/api/v1/responseActions/results HTTP/1.1
content-type: application/json
... (omitted) ...
{
  "type":"list",
  "direction":"past",
  "searchType":1,
  "count":100,
  "filter":[
    {"key":"actionStatus","ope":"MATCH","val":["running","ended"]},
    {"key":"executionHost","ope":"MATCH","val":["HOST185"]},
    {"key":"actionAcceptTime","ope":"TRANGE","val":["2023-10-25T12:00:0
0+09:00", "2023-10-30T12:00:00+09:00"]}
  ]
}
```

Response:

```
HTTP/1.1 200
content-type: application/json
... (omitted) ...
{
  "actionResult":[
    {
      "actionSid":"_JP1IMACTID_20f916e2-10d7/_JP1IMMHOST_HOST185//",
      "executionHost": "HOST185",
      "actionName": "act002",
      "actionType": "eventstatus",
      "executionCommand": {
        "dealt": 3,
        "eventSid":"_JP1IM_HOST185/_JP1IMSEQNO_8/_JP1IMEVBSEQNO_401"
      },
      "actionStatus": "ended",
      "targetSid": "_JP1IM_HOST185/_HOST_HOST185",
      "executionDeal": "manual",
      "executionDetailInfo": "jp1admin",
      "actionAcceptTime": "2023-10-27T15:26:50+09:00",
      "actionSendTime": "2023-10-27T15:26:50+09:00",
      "actionEndTime": "2023-10-27T15:26:50+09:00",
      "returnValue": "0",
      "executionResult": null,
      "message": null
    },
    ... (omitted) ...
  ],
  "beginData":"",
  "endData":"_JP1IMACTID_25e566fa-c54a/_JP1IMMHOST_HOST185//",
  "dbInfo":[
    {"beginData":"_JP1IMACTID_d9947fe1-23a5/_JP1IMMHOST_HOST185//",
     "endData":"_JP1IMACTID_20f916e2-10d7/_JP1IMMHOST_HOST185//",
     "since":"",
    },
    ... (omitted) ...
  ]
}
```

5.16.2 Manual execution of Response Action

Description

Operate responseAction(manual).

You can execute the following action type "commands:

- Execution of commands
- Execution of REST API
- Updating event status

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator

API version

v1

Format

Request line

```
POST /application/component/apiVersion/responseActions/manualExec httpVersion
```

Request message body

```
{
    "actionType":"Action type",
    "actionName":"Name of ResponseAction",
    "params":{"Parameters of ResponseAction"}
}
```

Parameters of ResponseAction

- When action type is set to "Remote command(cmd)"

```
    "params":{
        "host":"Execute Host name",
        "cmd":"Command",
        "envFile":" Environment variable file"
    }
```

- When action type is "REST API (restapi)"

```
    "params":{
        "method":"REST API methods",
        "url":"URL of REST API",
        "headers":"REST API request header",
        "body":"REST API request body"
    }
```

- When action type is "Event status updating (eventstatus)"

```
    "params":{
        "dealt":Event status,
        "eventSid":"JP1 Events SID,..."
    }
```

Response message body

```
{
  "actionSid":" ResponseAction SID",
  "warning":[
    {
      "messageId":"Message ID when a warning occurs",
      "message":"Message when a warning occurs"
    },
  :
  ]
}
```

Parameters

Here are the parameters that you specify for message body of the request:

Member name	Data type	Optional	Description
actionType	string	No	Specifies type of ResponseAction. One of the following value can be specified: If any other value is specified, error is returned. • cmd Execute remote command. • restapi Execute REST API

Member name	Data type	Optional	Description
			• eventstatus Execute updating event status of an event.
actionName	string	Yes	Specifies name of ResponseAction. The following value can be specified: If any other value is specified, error is returned. • 1 to 50 bytes. • All characters except the control character "ASCII code 0x00 to 0x1F,0x7F to 0x9F".
params	object	No	Specifies ResponseAction content. The parameters that you specify depend on type of ResponseAction. • For cmd See *For remote command (cmd)* table below. • For restapi See *For REST API(restapi)* table below. • For eventstatus See *For updating event status (eventstatus)* table below.

- For remote command (cmd)

Member name	Data type	Optional	Description
host	string	No	Specifies execute destination host name. Specify no more than 255 bytes. Otherwise, it is error.
cmd	string	No	Execute specifies OS command/parameter to be used. Specify no more than 4096 bytes. Otherwise, it is error.
envFile	string	Yes	Specify the absolute path of the file on the execution host that contains the environment variables to be read during command execution. Specify 255 bytes or less. Otherwise, it is error.

- For REST API(restapi)

Member name	Data type	Optional	Description
method	string	No	Specifies the method of REST API to execute. You can specify the following methods: Otherwise, it is error. • GET • HEAD • POST • PUT • PATCH • DELETE • OPTIONS • TRACE
url	string	No	Specifies URL of REST API to execute. The following value can be specified: Otherwise, it is error. • Specify 2046 bytes or less. • The characters that can be used are one-byte alphanumeric characters and the following symbols according to RFC2396. ";", "/", "?", ":", "@", "&", "=", "+", "$", ",", "-", "_", ".", "!", "~", "*", "'", "(", ")", "%" • Specify "http://" or "https://" at the beginning.
headers	object	No	Specifies the header of REST API to execute. Specify no more than 65,536 bytes. Otherwise, it is error.

Member name	Data type	Optional	Description
body	string	Yes	Specifies the body of REST API to execute. If you do not need a body, omit it. When specifying, specify a value less than 10MB. Otherwise, it is error.

- For updating event status (eventstatus)

Member name	Data type	Optional	Description
dealt	string	No	Specifies value of event status. You can specify value as follows: Otherwise, it is error. • 0:Unprocessed • 1:Processed • 2:Processing • 3:Hold
eventSid	string	No	Specifies SID of JP1 events. If you specify more than one event SID, concatenate the event SID with ",". You can specify up to 2,000 items. After that, it is error. The number of bytes must be less than 1MB. After that, it is error.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	--
400	KAJY64004-E	The content of execute requirement of ResponseAction is invalid. <Cause> • You are setting a value that cannot be set • Exceeded character limit • A parameter that cannot be omitted is omitted.
400	KAJY63321-E	JSON formatting of the request message body is invalid.
403	KAJY01000-E	You do not have execute permission for REST API.
500	KAJY63333-E	An unexpected error occurred in REST API processing.
500	KAJY64003-E	A error was returned from the destination ResponseAction execute control. <Cause> Execute of ResponseAction failed
500	KAJY64001-E	Execute destination cannot be obtained from the system configuration information. (There is no managed node of execute requesting host in the system configuration.)
		Execute destination could not be obtained from the system configuration information. (JP1/IM agent management base managing execute requesting host could not be obtained.)
500	KAJY64000-E	The system configuration information is not accessible.
500	KAJY64002-E	Communication with the destination ResponseAction execute control is not possible. <Cause> • Failed to communicate with ResponseAction execute control
500	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).

■About Warnings

If the acquisition of information from the non-executable action data table fails, the following message ID is output. The output destination is the warning object of the response when normal, and the warning object of extended information (extensions) when an error occurs.

Message ID	Description
KAJY63309-W	Cannot communicate with the response action result manage DB. <Cause> • Failed to connect the DB.
KAJY63310-W	Write error occurred at the response action result manage DB. <Cause> • Failed to operate reading DB.

Return values

- When the status code is 200

  If warning information is added to the response returned from the action execution request API, the warning information shown in the following table is added to this REST API response and returned to the request source.

  For the information to be returned, see ■*About Warnings* above.

Member name		Data type	Description
actionSid		string	Returns a unique ResponseAction SID within ResponseAction results-management DB.
warning		object[]	Object of the warning message.
	messageId	string	Returns message ID of the warning that occurred.
	message	string	Returns message of the warning that occurred.

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an Error occurs is returned. However, "returnCode" items are omitted.

  If warning information has been added to the response returned from execute request API of ResponseAction, the warning information shown in the following table is added to the "extensions" (extended information) field of message body of the response during error and returned to the request source.

Member name		Data type	Description
extensions		object[]	An object of extended information. Set the warning information that occurred.
	messageId	string	Returns message ID of the warning that occurred.
	message	string	Returns message of the warning that occurred.

Examples

Request:

- The following shows an example of using API when the command is executed.

```
POST http://hostname:20703/im/api/v1/responseActions/manualExec HTTP/1
.1
content-type: application/json
... (omitted) ...
{
  "actionType":"cmd",
  "actionName":"act001",
  "params":{
    "host":"HOST185",
    "cmd":"dir"
  }
}
```

- Here is an example of using API to execute a REST API using JP1 event-information:

```
POST http://hostname:20703/im/api/v1/responseActions/manualExec HTTP/1
.1
content-type: application/json
... (omitted) ...
{
  "actionType":"restapi",
  "actionName":"act001",
  "params":{
    "method":"GET",
    "url":"http://hostname:20703/im/api/version",
    "headers":"{}"
  }
}
```

- The following is an example of using API to change event status of an event to processed.

```
POST http://hostname:20703/im/api/v1/responseActions/manualExec HTTP/1
.1
content-type: application/json
... (omitted) ...
{
  "actionType":"eventstatus",
  "actionName":"act001",
  "params": {
    "dealt":1,
    "eventSid":"_JP1IM_HOST185/_JP1IMSEQNO_8/_JP1IMEVBSEQNO_401"
  }
}
```

Response:

```
HTTP/1.1 200 OK
content-type: application/json
...
{
  "actionSid": "_JP1IMACTID_cb82bd6d-6409/_JP1IMMHOST_HOST185//"
}
```

5.16.3 Convert event-takeover info

Description

Converts event takeover information.

Execution permissions

- JP1_Console_Admin
- JP1_Console_Operator

API version

v1

Format

Request line

```
POST /application/component/apiVersion/responseActions/eventsReplace httpVersion
```

Request message body

```
{
  "eventSid":"SID of JP1 event",
  "actionType":"Action type",
  "params":{"Parameters of ResponseAction"}
}
```

Response message body

```
{
"params":{"Parameters of ResponseAction"},
"results":{"Convert ResponseAction parameters"}
}
```

■ResponseAction parameters

- When action type" is set to "Remote command (cmd)"

```
    "params":{
        "host":"Execute host name",
        "cmd":"Command",
        "envFile":"Environment variable file"
    }
```

- When action type" is "REST API(restapi)"

```
    "params":{
        "method":"REST API Methods",
        "url":"URL of REST API",
        "headers":"REST API request header",
        "body":"REST API request body"
    }
```

- When action type" is "Updating event status of events (eventstatus)"

```
    "params":{
        "dealt":Event status,,
        "eventSid":"JP1 Events SID,..."
    }
```

- When action type" is "Jumping to the specified URL (jump)"

```
    "params":{
        "url":"Destination URL",
        "target":"Target-attributes of HTML"
    }
```

Parameters

Here are the parameters that you specify for message body:

Member name	Data type	Optional	Description
eventSid	string	No	Specifies SID of JP1 events for which you want to retrieve detailed information. For details about JP1 event SID, see *7.2.1(1) Event information object*. Specify a range of 1~512 bytes. Otherwise, it is error.
actionType	string	No	Specifies type" of ResponseAction. One of the following value can be specified: If any other value is specified, error is returned. • cmd Execute remote command. • restapi Execute REST API • eventstatus Execute updating event status of an event. • jump Displays/jumps to the specified URL
params	object	No	Specifies ResponseAction content. The parameters that you specify depend on type" of ResponseAction. • For cmd See *For remote command (cmd)* table below. • For restapi See *For REST API (restapi)* table below. • For eventstatus See *Updating event status of events (eventstatus)* table below. • For jump See *When displaying/jumping (jump) the specified URL* table below.

- For remote command (cmd)

Member name	Data type	Optional	Description
host	string	No	Specifies Execute destination Host name. Specify a range of 1~255 bytes. Otherwise, it is error.
cmd	string	No	Execute specifies OS command/parameter to be used. Specify a range of 1~4,096 bytes. Otherwise, it is error.
envFile	string	Yes	Specifies the absolute file path of file at execute destination, which contains the environment variables to be read during command execution. Specify a range of 1~255 bytes. Otherwise, it is error.

- For REST API (restapi)

Member name	Data type	Optional	Description
method	string	No	Specifies the method of REST API to execute. Specify 7 bytes or less. Otherwise, it is error.
url	string	No	Specifies URL of REST API to execute. Specify a range of 1~2,046 bytes. Otherwise, it is error.
headers	object	No	Specifies the header of REST API to execute. Specify a range of 1~65,536 bytes. Otherwise, it is error.
body	string	Yes	Specifies the body of REST API to execute. If you do not need a body, omit it. If specified, specify a range of less than 1~10MB. Otherwise, it is error.

- Updating event status of events (eventstatus)

Member name	Data type	Optional	Description
dealt	int	No	Specifies value of event status. Specify with a range of 0~3. Otherwise, it is error.
eventSid	string	No	Specifies SID of JP1 events. To specify multiple event SIDs, consolidated the event SIDs with ",". You can specify up to 2000 records. Specify 1 or more, less than 1MB. Otherwise, it is error.

- When displaying/jumping (jump) the specified URL

Member name	Data type	Optional	Description
url	string	No	Specify URL to jump to. Specify a range of 1~2,046 bytes. Otherwise, it is error.
target	string	Yes	Specifies the target attribute. Specify a range of 1~64 bytes. Otherwise, it is error.

Status codes

The following shows the status codes that are returned in response. For details about message, see the *JP1/Integrated Management 3 - Manager Messages*.

Status code	Message	Description
200	--	--
403	KAJY01000-E	You do not have execute permission for REST API.
400	KAJY63328-E	REST API parameter was specified incorrectly. The reason is that a parameter that cannot be omitted is omitted.
400	KAJY63329-E	JSON formatting of the request message body is invalid.
400	KAJY63330-E	The maximum number of bytes that can be specified was exceeded as a result of event inheritance information conversion processing.
500	KAJY63332-E	An error was returned in response from event detail info retrieval API.
500	KAJY63333-E	An unexpected error occurred in REST API processing.
500	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).

Return values

The following parameters are returned in response.

Member name	Data type	Description
params	object	Returns the parameters after event inheritance information conversion processing. Return in the same format as the parameterized "params". For details about parameter, see params in the parameter tables.
results	object	Returns the event takeover data conversion result corresponding to the above "params" parameters. Parameters that are omitted are not returned. Value returned by this parameter is as follows: • 0 Normal termination. • 1 Upper limit value was exceeded due to variable-transformation. • 2 The attribute corresponding to the variable does not exist. • 3

Member name	Data type	Description
		Attribute value of the corresponding property is an empty string. • 4 The encoding specification format for the variable is invalid.

The response to error is in the format described in *5.2.6 Error response message* when an error occurs, but "returnCode" is omitted. Extended information "extensions" assigns the same parameters as the response. However, if error processing occurs before event-takeover information conversion processing, omit this item.

■Extended info (extensions) parameters

```
{
  "timestamp":1539923958358,
  "status":400,
  ...Abbreviated...
  "extensions":{
    "params":{"Parameters of ResponseAction"},
    "results":{"Convert ResponseAction parameters"}
  }
}
```

Examples

The following shows how to execute a command.

Request:

```
POST http://hostname:20703/im/api/v1/responseActions/eventsReplace HTTP
/1.1
content-type: application/json
... (omitted) ...
{
  "eventSid":"_JP1IM_HOST185/_JP1IMSEQNO_8/_JP1IMEVBSEQNO_401",
  "actionType":"cmd",
  "params":{
    "host":"${event:EVHOST:}",
    "cmd":"dir",
    "envFile":"C:\\tmp\\envFile.txt"
  }
}
```

Response:

```
HTTP/1.1 200 OK
content-type: application/json
...
{
  "params": {
    "host": "HOST185",
    "cmd": "dir",
    "envFile": "C:\\tmp\\envFile.txt"
  },
  "results": {
  "host": 0,
  "cmd": 0,
  "envFile": 0
  }
}
```

5.17 API for definition file manipulation

5.17.1 Get definition file list

Description

Retrieves a list of defined file for a JP1/IM - Manager or JP1/IM - Agent.

Execution permissions

Following permissions are required:

When specify "Manager" at hostCategory

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

When specify "Agent" at hostCategory

- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/fileOperation/getFileList httpVe
rsion
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
[
  "hostCategory":"host type",
  "managerHostName":"Defined file list destination agent host-managed d
estination manger host name",
  "agentHostName":"Defined file list destination agent host name"
]
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter	Optional	Description
hostCategory	No	Specify "Manager" or "Agent" as host type. Performs an action on the defined file of the specified host type.
managerHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. Assuming that your host is the manager host for JP1/IM, get a list of file defined for the manager host in JP1/IM. • When hostCategory is "Agent" Specifies the manager Host name of JP1/IM that manages agent to which File list is to be acquired, from 1 to 255.
agentHostName	See *Description* column	• When hostCategory is "Manager"

Parameter	Optional	Description
		Ignores the specified item. - When hostCategory is "Agent" Specifies agent host of file list destination, in the range of 1 to 255.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
	KAJY02058-W	The format of the user-created definition file list definition file is incorrect.
	KAJY68102-W	The file described in the user-created definition file list definition file does not exist. The application-supplied File does not exist.
	KAJY68103-W	The length of file or file path exceeds the maximum.
		There are no required settings.
		The category name is invalid (the length of the string exceeds the upper limit or begins with "jp1_").
		The length of the character string for the definition import operation exceeds the upper limit.
		A file is specified that cannot be defined in the user-created definition file list definition file.
	KAJY68126-W	JP1/IM agent control base encountered a warning.
400	KAJY68101-E	Request parameter is invalid.
	KAJY68205-E	- Integrated agent host name specified in the request does not exist in JP1/IM - Manager - Logged in as does not have read/manipulate permissions for integrated agent specified in the request - The information of the integration agent or the host specified in the request is not in the unified agent host management DB
403	KAJY01000-E	The privilege of the user used for authentication is insufficient.
500	KAJY68104-E	JP1/IM agent control base encountered an error.
	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base.
	KAJY68212-E	Cannot connect to JP1/IM agent base.
	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Return values

- When the status code is 200

  Message body of the response returns the auto ResponseAction definition object described in *7.2.4(1) Auto Response Action definition Object*.

  For the format of the data, see *3.6.5 (1) Function for obtaining list of definition files* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. The parts that differ from JP1/IM - Agent are shown below.

Member name	Description
errfilelist:message	Describes message ID and message body of the error message. If it succeeds, omit this item.

Member name	Description
	Setup message of KAJY68102-W,KAJY68103-W.
message:errmessage	Describes message ID and message body of the error message. If successful, omit message entry. Setup message of KAJY02058-W.

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an error occurs is returned.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/fileOperation/getFileList  HTTP/1
.1
Authorization:Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJME
9qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ01lDQWdJQ
0FnSUNBZ01lDQWdJQ0Fn
Accept-Language: ja
Content-Type: application/json
Content-Length: 1024000
Accept: application/json
{
  "hostCategory":"Agent",
  "managerHostName":"immanager",
  "agentHostName":"imagent"
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type:application/json
... (omitted) ...

{
  "filelist":[
    {
      "filename": "jpc_alertmanager.yml",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf",
      "filecategoryID": "jp1_imagent",
      "filecategoryName": "jp1_imagent",
      "updatetime": "2023-07-21T10:23+09:00",
      "updateaction": "jp1ima\\addon_management\\alertmanager\\addon_jp
c_service_reload.bat"
    }, ...
  ],
"errfilelist":[
    {
      "filename": "file_sd_config_test.yml",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf",
    }, ...
  ]
}
```

5.17.2 Get definition file

Description

Retrieves JP1/IM - Manager or JP1/IM - Agent defined File.

Execution permissions

Following permissions are required:

When specify "Manager" at hostCategory

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

When specify "Agent" at hostCategory

- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/fileOperation/getFile httpVersi
on
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
[
  "filelist":[
    {
      "filename": "File Name",
      "filepath": "absolute path of File"
    }, ...
  ],
  "hostCategory":"host type",
  "managerHostName":"Defined file destination agent host management des
tination manger host name",
  "agentHostName":"Defined file destination Agent host name"
]
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter	Optional	Description
filename	No	Specifies file name.
filepath	No	Specifies the absolute location of file. If the absolute path including file name in file path exceeds 200 characters, the result is error.
hostCategory	No	Specify "Manager" or "Agent" as host type. Performs an action on the defined file of the specified host type.
managerHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. Assuming that your host is the manager host for JP1/IM, obtain file of the manager host for JP1/IM.

Parameter	Optional	Description
		• When hostCategory is "Agent" Specifies the manager host name of JP1/IM that manages agent to which file is to be acquired, from 1 to 255.
agentHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. • When hostCategory is "Agent" Define file specifies agent host to retrieve from, in the range of 1 to 255.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68105-E	Request parameter is invalid.
	KAJY68205-E	• Integrated agent host name specified in the request does not exist in JP1/IM - Manager • Logged in as does not have read/manipulate permissions for integrated agent specified in the request • The information of the integration agent or the host specified in the request is not in the unified agent host management DB
403	KAJY01000-E	The privilege of the user used for authentication is insufficient.
500	KAJY68104-E	JP1/IM agent control base encountered an Error.
	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base.
	KAJY68212-E	Cannot connect to JP1/IM agent base.
	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

If the definition file that you want to retrieve does not exist and you can create a compressed definition file (if you try to retrieve more than one file and some files do not exist), you can find file that failed to retrieve in definition file properties file in the compressed zip file.

Response

If the status code is 200, the file data of the definition file compressed in zip format is returned to the response body.

As a response header, setup the following:

```
Content-Type:application/zip
Content-Disposition: attachment; filename="File name of definition file co
mpressed in zip format"
```

The other response headers are the same as API's common spec. For the response header of common spec of API, see *5.2.5(2) Response header*.

Return values

- When the status code is 200

  In message body of the response, the file data of the definition file compressed in zip format is returned.

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an error occurs is returned.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/fileOperation/getFile  HTTP/1.1
Authorization:Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJME
9qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJQ
0FnSUNBZ0lDQWdJQ0Fn
Accept-Language: ja
Content-Type: application/json
Content-Length: 1024000
Accept: application/zip
{
  "filelist":[
    {
      "filename": "jpc_imagent.json",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf",
    }, ...
  ],
  "hostCategory":"Agent",
  "managerHostName":"immanager",
  "agentHostName":"imagent"
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type:application/zip
Content-Disposition: attachment; filename="C:\Program Files\Hitachi\jp1
ima\tmp\upload\imagenthost_UUID.zip"
... (omitted) ...
```

5.17.3 Delete definition file

Description

Delete JP1/IM - Manager or JP1/IM - Agent definition file.

Execution permissions

Following permissions are required:

When specify "Manager" at hostCategory

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

When specify "Agent" at hostCategory

- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/fileOperation/deleteFile httpVer
sion
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
[
  "filelist":[
    {
      "filename": "File Name",
      "filepath": "absolute path of File",
      "updateaction": "Manipulation for defining import"
    }, ...
  ],
  "hostCategory":"host type",
  "managerHostName":"Definition file delete destination agent host mana
gement destination manger host name",
  "agentHostName":"Definition file delete destination Agent host name"
]
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter	Optional	Description
filename	No	Specifies File.
filepath	No	Specifies the absolute location of file. If the absolute path including file name in file path exceeds 200 characters, the result is error.
updateaction	Yes	Specifies a value from 1 to 4096 bytes that should be executed when file is updated.
hostCategory	No	Specify "Manager" or "Agent" as host type. Performs an action on the defined file of the specified host type.
managerHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. Delete file of the manager host in JP1/IM, assuming that the local host is the manager host in JP1/IM. • When hostCategory is "Agent" Specify a value from 1 to 255 bytes for the JP1/IM manager host name that manages the agent from which the definition file is to be deleted.
agentHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. • When hostCategory is "Agent" Specify the agent host name of the definition file deletion destination with 1 to 255 bytes.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
	KAJY68126-W	JP1/IM agent control base encountered a warning.
400	KAJY68107-E	Request parameter is invalid.
	KAJY68205-E	• Integrated agent host name specified in the request does not exist in JP1/IM - Manager

Status code	Message	Description
		• Logged in as does not have read/manipulate permissions for integrated agent specified in the request • The information of the integration agent or the host specified in the request is not in the unified agent host management DB
403	KAJY01000-E	The privilege of the user used for authentication is insufficient.
500	KAJY68104-E	JP1/IM agent control base encountered an error.
	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base.
	KAJY68212-E	Cannot connect to JP1/IM agent base.
	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Response

If the status code is 200, the following is returned to the response body in JSON format:

```
{
  "filelist":[
    {
      "filename": "File name",
      "filepath": "absolute path of File",
      "result": "Result of file deletion",
      "message": "Message"
    }, ...
  ]
}
```

Member name	Description
filename	Describes file name.
filepath	Describes the absolute path where file will be placed.
result	Describes the outcome of file deletion. See *Table 5-15* for the character strings to be described.
filelist:message	Provides the error message ID and its body if the action for file deletion fails. If it succeeds, omit this item. If result is recovery fail, the error message in the table indicates message when the import operation failed.

Table 5–15: Contents of the result

Delete for file	Operations for importing definition	Recovery process	Content of result
Y	Y	--	success
N	--	--	delete fail
Y	N	Y	action fail
Y	N	N	recovery fail

Legend

Y: Succeeded, N: Failed, --: No processing

Return values

- When the status code is 200

  None

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an error occurs is returned.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/fileOperation/deleteFile HTTP/1.1
Authorization:Bearer anAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJME
9qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJQ
0FnSUNBZ0lDQWdJQ0Fn
Accept-Language: ja
Content-Type: application/json
Content-Length: 1024000
Accept: application/json
{
  "filelist":[
    {
      "filename": "user_file_sd_config_test.yml",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf\\user",
      "updateaction": "jp1ima\\addon_management\\alertmanager\\addon_jp
c_service_reload.bat"
    }, ...
  ],
  "hostCategory":"Agent",
  "managerHostName":"immanager",
  "agentHostName":"imagent"
}
```

Response:

```
HTTP/1.1 200 OK
Content-Type:application/json
... (omitted) ...

{
  "filelist":[
    {
      "filename": "user_file_sd_config_test.yml",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf\\user",
      "result": "delete fail",
      "message": "KAJY68126-W A warning occurred in the integrated agen
t control platform. (detailed-information : KNBC20015-W Failed to delet
e a definition file. (details = target file does not exist. filename=C:
\\Program Files\\Hitachi\\jp1ima\\conf\\user\\user_file_sd_config_test.
yml))"
    }, ...
  ]
}
```

Notes

- After deletion of the definition File, the service might be restart because of import of the definition information.

- If the service startup fails after deletion of file, the system performs a recovery operation. However, if the recovery operation fails, status might be the one in which the service was stopped.
- In a clustered configuration, a deletion of the defined file might cause a failover. Also, you cannot start the service at the failover destination, and the failover might fail. Depending on the load condition, restart and recovery process of the service may take a long time. In the case of a cluster configuration, the cluster software may judge it to be abnormal and cause a failover. For this reason, file's deletion should be performed during system-maintenance hours.

5.17.4 Updated definition file

Description

Update JP1/IM - Manager or JP1/IM - Agent definition file.

Execution permissions

Following permissions are required:

When specify "Manager" at hostCategory

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

When specify "Agent" at hostCategory

- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/fileOperation/updateFile httpVer
sion
```

Request header

```
Authorization:BeareranAxYWRtaW46TUdGa01tTTJNMlV3TURFNFh6STNYekE0T2pJME9
qTXpYMTlmWDE5ZlgxOWZYMTlmWDE5ZlgycHdNV0ZrYldsdUlDQWdJQ0FnSUNBZ0lDQWdJQ0
FnSUNBZ0lDQWdJQ0Fn
Accept-Language: ja
```

Follow the request header in *5.2.3 Request format*.However, Content-Type has the following format:

```
Content-Type: multipart/form-data; boundary=-----5a6a576p44OV44Kh44Kk44
Or5pu05paw
Content-Length: 1024000
Accept: application/json
```

Request message body

```
[
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="hostCategory"

"Host type"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="managerHostName"
"Definition file destination agent host management destination Manger h
ost name"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="agentHostName"

"Definition file destination agent host name"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="file"; filename="/C:/Users/xxxxx/
Desktop/sample.zip"
Content-Type: application/zip

zip data
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
]
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter	Optional	Description
filename	No	Specifies the absolute path to file named after zip has been compressed. File number must be between 1 and 200 bytes. Does not check the file size limit and checks the request body size limit.
hostCategory	No	Specify "Manager" or "Agent" as host type. Performs an action on the defined file of the specified host type.
managerHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. Assuming that your host is the manager host for JP1/IM, refresh file of the manager host in JP1/IM. • When hostCategory is "Agent" Specify a value from 1 to 255 bytes for the JP1/IM manager host name that manages the agent to which the definition file is to be updated.
agentHostName	See *Description* column	• When hostCategory is "Manager" Ignores the specified item. • When hostCategory is "Agent" Specify the agent host name of the definition file update destination with 1 to 255 bytes.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
	KAJY68126-W	JP1/IM agent control base encountered a warning.
400	KAJY68111-E	Request parameter is invalid.
	KAJY68205-E	• Integrated agent host name specified in the request does not exist in JP1/IM - Manager • Logged in as does not have read/manipulate permissions for integrated agent specified in the request • The information of the integration agent or the host specified in the request is not in the unified agent host management DB
403	KAJY01000-E	The privilege of the user used for authentication is insufficient.
500	KAJY68104-E	JP1/IM agent control base encountered an error.

Status code	Message	Description
	KAJY00009-E	Request body limit exceeded.
	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base.
	KAJY68212-E	Cannot connect to JP1/IM agent base.
	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Response

If the status code is 200, the following is returned to the response body in JSON format:

```
{
  "filelist":[
    {
      "filename": "File name",
      "filepath": "File's absolute path",
      "result": "Updating file result",
      "message": "Message"
    }, ...
  ]
}
```

Member name	Description
filename	Describes file name.
filepath	Describes the absolute path where file will be placed.
result	Describes the outcome of file updating. See *Table 5-16* for the strings to be described.
filelist:message	Provides the error message ID and its body if file refresh attempt fails. If it succeeds, omit this item. If result is recovery fail, the error message in the table indicates message when the import operation failed.

Table 5–16: Contents of the result

Overriding File	Operations for importing definition	Recovery process	Content of result
Y	Y	--	success
N	--	--	update fail
Y	N	Y	action fail
Y	N	N	recovery fail

Legend

Y: Succeeded, N: Failed, --: No processing

Return values

- When the status code is 200

  None

- When the status code is other than 200

  In message body of the response, the exception object in the response format described in *5.2.6 Error response message* when an error occurs is returned.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/fileOperation/updateFile HTTP/1.1
Content-Type: multipart/form-data;boundary=-----5a6a576p44OV44Kh44Kk44O
r5pu05paw
[
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="hostCategory"

"Agent"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="managerHostname"

"immanager"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="agentHostname"

"imagent"
-----5a6a576p44OV44Kh44Kk44Or5pu05paw
Content-Disposition: form-data; name="file"; filename="/C:/Users/xxxxx/
Desktop/sample.zip"
Content-Type: multipart/form-data; boundary=-----5a6a576p44OV44Kh44Kk44
Or5pu05paw
zip data
-----5a6a576p44OV44Kh44Kk44Or5pu05paw--
]
```

Response:

```
HTTP/1.1 200 OK
Content-Type:application/json
... (omitted) ...

{
  "filelist":[
    {
      "filename": "user_file_sd_config_test2.yml",
      "filepath": "C:\\Program Files\\Hitachi\\jp1ima\\conf\\user",
      "result": "update fail",
      "message": "KAJY68126-W A warning occurred in the integrated agen
t control platform. (detailed-information : KNBC20020-W Failed to updat
e a definition file. (details = specified file not included in user-def
inition file list file. filename=C:\\Program Files\\Hitachi\\jp1ima\\co
nf\\user\\user_file_sd_config_test2.yml))"
    }, ...
  ]
}
```

Notes

- Prior to updating file definition, make sure that the definition file format, character code, etc. are correct manually. If file is invalid, updating might fail. If updating of the defined file fails, an JP1 event is sent. Check the details of JP1 event that occurred and take appropriate action.
- Some services are automatically restarted when file is updated.

The monitoring operation may be temporarily stopped by restart of the service. Also, in a clustered configuration, a setup# in outage detection times for the monitored services in the cluster software might cause a failover. Therefore, you should refresh file during system-maintenance hours.

#

The estimate of the stop detection time depends on the machine specification and the load condition. However, since the service is restarted for each update of one definition file, consider that it is about one minute for each definition file.

For example, if you are updating 10 files at the same time, set setup for the cluster software shutdown detection period to 10 minutes.

If you cannot increase the detection time, do not use the definition file manipulation feature and login the host. Then, refresh the direct definition file.

5.18 API for Integrated agent Administration

5.18.1 Retrieve integrated agent info

Description

This API is used to obtain integrated agent data.

If an office or relay manager exists under the control of Integrated manager, integrated agent under the control of the office or relay manager is also acquired.

If JP1 user you login has read permission, get agent info.

Execution permissions

JP1_Console_Admin

API version

v1

Format

Request line

```
POST /im/api/v1/agents httpVersion
```

Request message body

None

Response message body

```
{
  "agents": [
    Integrated agent info Object, ...
  ],
  "messageList":[
    {
      "messageId": Message ID,
      "message": Message
    }, ...
}
```

Parameters

None

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
403	KAJY01000-E	The permission of the user used for authentication is insufficient.
200	KAJY68500-W	Unable to connect to the manager's integrated agent host administration DB. If you are unable to connect to integrated agent host administration DB of more than one administration manager, specify host name with a concatenation of ",".

Status code	Message	Description
200	KAJY68204-W	Cannot connect to the manager's Intelligent Integrated Management Base. If you are unable to connect to Intelligent Integrated Management Base of more than one manager, specify host name with a concatenation of ',' for each manager.
200	KAJY68210-W	Intelligent Integrated Management Base operation encountered an error.
500	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Return values

The following table describes the return value.

Parameter name	Data type	Optional	Description
`agents`	object[]	No	Specifies an array of integrated agent info objects. If integrated agent does not exist, specify an empty array.
`Integrated agent info object`	object	Yes	See *7.2.5(1) Integrated agent Info object*.
`messageList`	object	Yes	Message specifies an array of objects. If Message does not exist, it is omitted.
`messageId`	string	No	Specify message ID.
`message`	string	No	Specify message body. The language used is determined by Accept-Language property specification in HTTP request header.

Examples

Request:

```
POST http://hostname:20703/im/api/v1/agents
```

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
{
     "agents": [
          {
               "agentid": "RENEMzNENDg5RkQyNEM2OT",
               "hostname": "agenthostA",
               "os": "windows",
               "installpath": "\\Program Files\\Hitachi\\jp1ima",
               "imversion": "130000",
               "managerhost": "managerhostA",
               "registeredtime": "2020-03-01T00:00:00Z",
               "addons": [
                    {
                         "addonName": "Windows metric collector(Window
s exporter)",
                         "enables": true
                    }
               ]
          }
```

```
    ]
}
```

5.18.2 Delete integrated agent info

Description

This API is used to delete the specified integrated agent.

You can Delete a integrated agent for which JP1 user who Login has read/write access.

Execution permissions

JP1_Console_Admin

API version

v1

Format

Request line

```
POST /im/api/v1/agents/delete httpVersion
```

Request message body

```
{
  "agents": [
    {
      "agenthost": integrated agent host name,
      "managerhost": manager host name
    }, ...
  ]
}
```

Response message body

If successful, there is no response.

If the warning ends, the following response is returned.

```
{
    "errhostlist":[
        {
            "agenthost": integrated-agent-hostname,
            "managerhost": manager-hostname
        }, ...
    ]
    "messageList":[
        {
            "messageId": Message ID,
            "message": Message
        }, ...
    ]
}
```

Parameters

Here are the parameters that you specify for message body:

Parameter name	Data type	Optional	Description
`agents`	object[]	No	Specifies the Unified Agent to delete. You can specify up to 200 integrated agents. An empty array cannot be specified.
`agenthost`	string	No	Specify host name of integrated agent, from 1 to 255.
`managerhost`	string	No	Specifies the manager host name from 1 to 255 bytes.

Response

Parameter name		Data type	Optional	Description
`errhostlist`		object[]	Yes	The array is populated with the Unified Agents that failed to be deleted. If there are no failed hosts, it is omitted.
	`agenthost`	string	No	Hostname of the integrated agent is set.
	`managerhost`	string	No	Manager hostname is set.
`messageList`		object	Yes	The array of message objects is populated. If the message does not exist, it is omitted.
	`messageId`	string	No	The message ID is set.
	`message`	string	No	The body of the message is set. The language used depends on what is specified in the Accept-Language property of the HTTP request header.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68201-E	API request is invalid. The process is turned stopped when one incorrect request is found.
200	KAJY68213-W	• Integrated agent host name specified in the request or the configuration managed by the manager host name does not exist in JP1/IM - Manager • Logged in as does not have read/manipulate permissions for integrated agent specified in the request • The information of the integration agent or the host specified in the request is not in the unified agent host management DB.
403	KAJY01000-E	The permission of the user used for authentication is insufficient.
500	KAJY68501-E	Unable to connect to integrated agent host admin DB for the specified integrated agent manager.
200	KAJY68500-W	Unable to connect to the Unified Agent Host Management DB for the specified subordinate manager.
200	KAJY68204-W	Cannot connect to Intelligent Integrated Management Base of the manager for the specified integrated agent.
200	KAJY68210-W	Intelligent Integrated Management Base operation encountered an error.

Return values

None

Examples

Request:

```
POST http://hostname:20703/im/api/v1/agents/delete
{
    "agents": [
      {
        "agenthost":"hostA",
        "managerhost":"hostB"
      }
    ]
}
```

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
```

5.18.3 Retrieve Secret List

Description

Get a list of secrets that JP1/IM agent control base manages.

Execution permissions

JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/agents/secrets httpVersion
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
[
  "agenthost":"integrated agent host name",
  "managerhost":"Manager host name"
]
```

Response message body

Returns a list of secrets. In this case, value of obfuscated and secret is an empty string.

```
{
    "secrets": [
        {
            "key": "Key1",
            "obfuscated": "",
            "secret": ""
        },
        {
            "key": "Key2",
            "obfuscated": "",
            "secret": ""
        },
        {
            "key": "Key3",
            "obfuscated": "",
            "secret": ""
        }
    ]
}
```

Parameters

Here are the parameters that you specify for message body:

Parameter name	Data type	Optional	Description
agenthost	string	No	Specify integrated agent host in the range of 1 to 255.
managerhost	string	No	Specify the manager host name in the range of 1 to 255.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68209-E	Request parameter is invalid.
400	KAJY68205-E	• Integrated agent host name specified in the request or the configuration managed by the manager host name does not exist in JP1/IM - Manager • Logged in as does not have read/manipulate permissions for integrated agent specified in the request
403	KAJY01000-E	The permission of the user used for authentication is insufficient.
500	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
500	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base of the manager for the specified integrated agent.
500	KAJY68207-E	JP1/IM agent base operation encountered an error.
500	KAJY68211-E	Intelligent Integrated Management Base operation encountered an error.
500	KAJY68212-E	Cannot connect to JP1/IM agent base.
500	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Return values

None

Examples

Request:

```
POST http://immhost01:20703/im/api/v1/agents/secrets
```

Manager host name: immhost01

```
{
    "agenthost": "hostA",
    "managerhost": "hostB"
}
```

Response:

Omitted

5.18.4 Add, update, delete the secrets

Description

Execute add, update, and delete of the secret that you want JP1/IM agent control base to manage.

You can register up to 1,000 secrets.

Execution permissions

JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/agents/secrets/change httpVersi
on
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

- Execute only add or refresh (Delete is not executed)

Write the secret that you want to add in "add".

```
[
    "agenthost":"integrated agent host name",
    "managerhost":"Manager host name",
    "add": {
        "secrets": [
            {
                "key": "key1",
                "secret": "Plaintext secret 1"
            },
            {
                "key": "key2",
                "secret": "Plaintext secret 2"
            },
            {
                "key": "key3",
                "secret": "Plaintext secret 3"
            }
        ]
    }
}
```

- If you want to execute only deletion (do not execute a add or refresh)

Write the secret that you want to delete in "delete".

```
[
    "agenthost":"integrated agent host name",
    "managerhost":"Manager host name",
    "delete": {
        "secrets": [
            {
                "key": "key1",
            },
            {
                "key": "key2",
            },
            {
                "key": "key3",
            }
        ]
    }
}
```

- To execute add or updating and deletion

Write add or the secret you want to renew on add and put the secret you want to delete on "delete".

If you specify the same key for "add" and "delete", "add" applies.

```
[
    "agenthost":"integrated agent host name",
    "managerhost":"Manager host name",
    "add": {
        "secrets": [
            {
                "key": "key1",
                "secret": "Plaintext secret 1"
            },
            {
                "key": "key2",
                "secret": "Plaintext secret 2"
            },
            {
                "key": "key3",
                "secret": "Plaintext secret 3"
            }
        ]
    },
    "delete": {
        "secrets": [
            {
                "key": "key1",
            },
            {
                "key": "key2",
            },
            {
                "key": "key3",
            }
        ]
    }
}
```

Response message body

None

Parameters

Here are the parameters that you specify for message body:

Parameter name		Data type	Optional	Description
agenthost		string	No	Specify integrated agent host in the range of 1 to 255.
managerhost		string	No	Specify the manager Host name in the range of 1 to 255.
add		object	Yes	Specifies the secret to add or refresh. If you do not have a secret to add or refresh, omit it.
	secrets	object[]	No	Specifies the secret to add or refresh.
	key	string	No	Specify the secret key for the key name. The number of characters that can be specified is 1 to 1024, and the number of characters that can be specified is ASCII (0x20 to 0x7e). Otherwise, it is error.
	secret	string	No	Specify a secret. The number of characters that can be specified is 1 to 1024, and the number of characters that can be specified is ASCII (0x20 to 0x7e). Otherwise, it is error.
delete		object	Yes	Specifies the secret to delete. If there is no secret to delete, omit it.
	secrets	object[]	No	Specifies the secret to delete.
	key	string	No	Specify the secret key for the key name. The number of characters that can be specified is 1 to 1024, and the number of characters that can be specified is ASCII (0x20 to 0x7e). Otherwise, it is error.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68209-E	Request parameter is invalid.
400	KAJY68205-E	• Integrated agent host name specified in the request or the configuration managed by the manager host name does not exist in JP1/IM - Manager • Logged in as does not have read/manipulate permissions for integrated agent specified in the request
403	KAJY01000-E	The permissions of the user used for authentication is insufficient.
500	KAJY00007-E	System error has occurred (out of disk, out of memory, etc.).
500	KAJY02039-E	An internal error occurred (such as an invalid API parameter or environmental error).
500	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base of the manager for the specified integrated agent.
500	KAJY68207-E	JP1/IM agent base operation encountered an Error.
500	KAJY68211-E	Intelligent Integrated Management Base operation encountered an error.

Status code	Message	Description
500	KAJY68212-E	Cannot connect to JP1/IM agent base.
500	KAJY68501-E	Unable to connect to the manager's unified agent host management DB.

Error message output

API response, including the content of the error message, is returned to the caller when an Execute of Error occurs. The caller displays Message at the caller, using the information of the received response.

Return values

None

Examples

Request:

```
POST http://immhost01:20703/im/api/v1/agents/secrets/change
```

Manager host name: immhost01

```
{
    "agenthost": "hostA",
    "managerhost": "hostB",
    "add": {
      "secrets": [
        {
          "key": "key1",
          "secret": "secret1"
        },
        {
          "key": "key2",
          "secret": "secret2"
        }
      ]
    }
}
```

Response:

Omitted

5.19 API for Lower manager Info Management

5.19.1 Retrieve lower manager info list

Description

Retrieves a list of base manager or relay manager under Integrated manager.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
GET /application/component/apiVersion/subManagers httpVersion
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

None

Response message body

```
{
    "subManagers": [
        hostname, ...
    ]
}
```

Parameters

None

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
403	KAJY01000-E	The permission of the user used for authentication is insufficient.
500	KAJY68501-E	Unable to connect to Unified Agent Host Management DB.

Return values

The following information is returned in the response body, if the status code is 200:

Member name	Data type	Optional	Description
subManagers	string[]	No	Specifies an array of host name for lower manager. Specify host name within the range of 1 to 255. An empty array cannot be specified.

Error message output

API response, including the content of the error message, is returned to the caller when an execution error occurs. The caller displays message at the caller, using the information of the received response.

Examples

Request:

```
GET http://immhost01:20703/im/api/v1/subManagers
```

Manager host name: immhost01

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
{
    "subManagers":["hostA"]
}
```

5.19.2 Add lower manager info

Description

Register the information of the base manager or relay subordinate manager under the integration manager.

If information for registered subordinate managers, if specified, is updated with that information.

Only hosts registered as subordinate hosts of Integration Manager in IM Configuration Management can be specified.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/subManagers/createInfo httpVersi
on
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
{
    "hostname": Host-name,
    "initialsecret": Initial-secret
}
```

Response message body

```
None
```

Parameters

Here are the parameters that you specify for message body:

Parameter name	Data type	Optional	Description
hostname	string	No	Specify host name of lower manager in the range of 1 to 255.
initialsecret	string	No	Specify initial secret. The number of characters that can be specified is 1 to 1024, and the number of characters that can be specified is ASCII (0x20 to 0x7e).

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68012-E	API request is invalid. The process is turned stopped when one bad request is found.
403	KAJY01000-E	The privilege of the user used for authentication is insufficient.
500	KAJY68501-E	Unable to connect to Unified Agent Host Management DB in Unified Agent Manager.
500	KAJY68203-E	Cannot connect to Intelligent Integrated Management Base on lower manager.
500	KAJY68017-E	Add of lower manager data has failed.

Return values

There is no response body.

Examples

Request:

```
POST http://immhost01:20703/im/api/v1/subManagers/createInfo
{
    "hostname":"hostA",
    "initialsecret": "XXXXXXXXXXX"
}
```

Manager host name: immhost01

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
```

5.19.3 Delete lower manager info

Description

Delete base manager or relay manager under Integrated manager.

Execution permissions

Following permissions are required:

- JP1 resource group: *
- JP1 permission level: JP1_Console_Admin

API version

v1

Format

Request line

```
POST /application/component/apiVersion/subManagers/deleteInfo httpVersion
```

Request header

Follow the request header in *5.2.3 Request format*.

Request message body

Message body of the request can be sent in JSON formats.

```
{
    "subManagers":[
        hostname, ...
    ]
}
```

Response message body

If successful, there is no response.

If the warning ends, the following response is returned.

```
{
    "errhostlist":[
        hostname, ...
    ],
    "messageList":[
        {
            "messageId": Message ID,
            "message": Message
        }, ...
    ]
}
```

Parameters

Here are the parameters that you specify for message body of the request:

Parameter name	Data type	Optional	Description
`subManagers`	string[]	No	Specifies an array of host name for lower manager. Specify host name within the range of 1 to 255. An empty array cannot be specified.

Status codes

The following table describes the status codes that are returned as a response to the request:

Status code	Message	Description
200	--	API operation was successful.
400	KAJY68013-E	API request is invalid. The process is turned stopped when one bad request is found.
403	KAJY01000-E	The permission of the user used for authentication is insufficient.

Status code	Message	Description
500	KAJY68501-E	Unable to connect to Integration agent host management DB for Integration Manager.
200	KAJY68500-W	Cannot connect to integrated agent host administration DB of lower manager. If you are unable to connect to integrated agent administration DB of more than one administration manager, host name contains a concatenation of the administration managers host name with ",".
200	KAJY68204-W	Cannot connect to Intelligent Integrated Management Base on lower manager. If you are unable to connect to Intelligent Integrated Management Base of more than one manager, host name will contain a concatenation of the respective manager host name with ",".
200	KAJY68016-W	Lower manager data does not exist.
200	KAJY68018-W	Delete of lower manager data has failed.

Return values

Parameter name		Data type	Optional	Description
`errhostlist`		`string[]`	`Yes`	Sets an array of host names of subordinate managers that failed to delete. If there are no failed hosts, it is omitted.
`messageList`		`object`	`Yes`	The array of message objects is populated. If the message does not exist, it is omitted.
	`messageId`	`string`	No	The message ID is set.
	`message`	`string`	No	The body of the message is set. The language used depends on what is specified in the Accept-Language property of the HTTP request header.

Examples

Request:

```
POST http://immhost01:20703/im/api/v1/subManagers/deleteInfo
{
    "subManagers":["hostA"]
}
```

Manager host name: immhost01

Response:

```
< HTTP/1.1 200 OK
< Content-Type: application/json
{
    "errhostlist":[
      "hostA"
    ],
    "messageList":[
        {
            "messageId":"KAJY68500-W",
            "message": "The Intelligent Integrated Management Base DB c
annot be connected to.(JP1/IM-Manager hostname : hostA)"
        }
    ]
}
```

5.20 API for Prometheus server operation

Describes operations related to Prometheus server operation-related API.

5.20.1 Reload Prometheus server

Description

Reloads Prometheus server definition files (jpc_prometheus_server.yml, jpc_alerting_rules.yml, file discovery definition files, etc.) and reflects them in the operation of Prometheus server.

Reloading the Prometheus server is faster than restarting the Prometheus server and maintains the state at the time of notification failure.

Special Notes on API Operation

- All definition fields are reloaded.
- If you change the threshold of an alert rule and reload, the status of the alert changes to the status corresponding to the changed threshold.
- If you reload an incorrect definition file, all definition entries will not be updated. It is recommended that you use the `promtool check config` command to check the format of the configuration file before reloading.

Format

Request line

```
POST /-/reload HTTP/1.1
```

Request header

Header Name	Setting Value
Host	Specify the information of the host of the Prometheus server to which the API is connected as a header value in the following format. Host name or IP address: Port number ":port number" is optional. • Host name or IP address Specify the host name or IPv4 address of the Prometheus server. • Port number Specifies the port number to use when connecting to the Prometheus server. This header is optional.

Request message body

None

Response message body

If the reload is successful, there is no response.

If the reload fails, a message (the value printed by the Prometheus server) is set indicating the cause of the failure.

Status codes

Status code	Message	Description
200	OK	Reloaded successfully.
Other than 200	Other than OK	Reloaded successfully.

Examples

The following is an example of using this API using the OSS curl command.

On successful reload:

```
>curl --request POST "http://localhost:20713/-/reload"

>
```

On reload failure:

```
>curl --request POST "http://localhost:20713/-/reload"
failed to reload config: couldn't load configuration (--config.file="C:\\j
p1pccs\\conf\\jpc_prometheus_server.yml"): parsing YAML file C:\\jp1pccs\\
conf\\jpc_prometheus_server.yml: yaml: unmarshal errors:
  line 10: field test not found in type config.plain
>
```

5.20.2 Prometheus server health check

Description

Perform a health check on the Prometheus server.

The status code always returns 200.

Format

Request line

```
GET /-/healthy HTTP/1.1
```

Request header

Header Name	Setting Value
`Host`	Specify the information of the host of the Prometheus server to which the API is connected as a header value in the following format. Host name or IP address: Port number ":port number" is optional. • Host name or IP address Specify the host name or IPv4 address of the Prometheus server. • Port number Specifies the port number to use when connecting to the Prometheus server. This header is optional.

Request message body

None

Status codes

Always return 200.

Examples

The following is an example of using this API using the OSS curl command.

If the Prometheus server is working properly:

```
>curl -I --request GET "http://localhost:20713/-/healthy"
HTTP/1.1 200 OK
```

```
Date: Sat, 07 Aug 2021 01:20:57 GMT
Content-Length: 23
Content-Type: text/plain; charset=utf-8
>
```

If the Prometheus server is not working properly:

```
>curl -I --request GET "http://localhost:20713/-/healthy"
curl: (7) Failed to connect to localhost port 20713: Connection refused
>
```

5.21 API for Alertmanager operation

Describes operations related to Alertmanager operation-related API.

5.21.1 Reload Alertmanager

Description

Reload the Alertmanager definition file (jpc_alertmanager.yml) and reflect it in the operation of Alertmanager.

Reloading Alertmanager is faster than restarting Alertmanager and maintains the state it was in when the notification failed.

Special Notes on API Operation

- All definition fields are reloaded.
- If you leave an alert in a normal state and change the threshold of the alert rule to become unhealthy, the alert becomes unhealthy.
- If you leave an alert in an abnormal state and change the threshold of the alert rule to become normal, the alert becomes normal.
- If you reload an incorrect definition file, all definition entries will not be updated.

Format

Request line

```
POST /-/reload HTTP/1.1
```

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*`:`*Port number* "`:`*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Response message body

If the reload is successful, there is no response.

If the reload fails, a message indicating the cause of the failure (the value output by Alertmanager) is set.

Status codes

Status code	Message	Description
200	OK	Reloaded successfully.
Other than 200	Other than OK	Reload failed.

Examples

The following is an example of using this API using the OSS curl command.

On successful reload:

```
>curl --request POST "http://localhost:20714/-/reload"

>
```

On reload failure:

```
>curl --request POST "http://localhost:20714/-/reload"
failed to reload config: yaml: line 11: could not find expected ':'
>
```

5.21.2 Alertmanager health check

Description

Perform a health check of Alertmanager.

The status code always returns 200.

Format

Request line

```
GET /-/healthy HTTP/1.1
```

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*:*Port number* ":*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Status codes

Always return 200.

Examples

The following is an example of using this API using the OSS curl command.

If Alertmanager is working properly:

```
>curl -I --request GET "http://localhost:20714/-/healthy"
HTTP/1.1 200 OK
Date: Sat, 07 Aug 2021 01:20:57 GMT
Content-Length: 23
Content-Type: text/plain; charset=utf-8
>
```

If Alertmanager is not working properly:

```
>curl -I --request GET "http://localhost:20714/-/healthy"
curl: (7) Failed to connect to localhost port 20714: Connection refused
>
```

5.21.3 Get silence list of Alertmanager

Description

Gets the list of silences created in Alertmanager in JSON format.

Format

Request line

```
GET /api/v2/silences HTTP/1.1
```

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*:*Port number* ":*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Response message body

```
[
    {
        "id": "Silence ID",
        "status": {
            "state": "status"
        },
        "updatedAt": "Updated",
        "comment": "comment",
        "createdBy": "Author Name",
        "endsAt": "End date and time",
        "matchers": [
            {
                "isRegex":regular expression flag,
                "name": "label name",
                "value": "value"
            },
            ...
        ],
        "startsAt": "Start date and time"
    },
        ...
]
```

Response parameters

Member name		Data type	Description
id		string	Sets an ID that is uniquely assigned to the silence configuration. Used to run the Silence Revocation API. Alertmanager configures it automatically.
status		object	An object that represents the silence state. Alertmanager configures it automatically.
	state	string	One of the following values is set: • active The silence setting is enabled. • pending The application start date and time has not passed. • expired The application end date and time has passed. Alertmanager configures it automatically.
updatedAt		string	The creation or modification date and time of the silence configuration is set in the ISO8601 extended format. Alertmanager configures it automatically.
matchers		object	Conditions are set to suppress the issuance of alerts. Suppresses the issuance of alerts that match the label name and label value specified by name and value.
	name	string	The label name is set.
	value	string	The value of the label is set.
	isRegex	boolean	Sets whether the value of value is specified by regular expression. • true It is specified by a regular expression. • false Not specified in a regular expression.
	isEqual	boolean	Set whether to suppress alert notifications when matchers are met. Always set to "true" (suppress alert notifications). Alertmanager configures it automatically.
startsAt		string	The date and time when silence is applied is set in the ISO8601 extended format. The date and time will be the time zone specified in the "Create Silence" API.
endsAt		string	The silence end date and time is set in the ISO8601 extended format. The date and time will be the time zone specified in the "Create Silence" API.
createdBy		string	Sets the author name of the silence configuration.
comment		string	The comment for the silence settings is set.

Status codes

Status code	Message	Description
200	OK	The list of silences was successfully obtained.
Other than 200	Other than OK	Failed to get silence list.

Examples

The following is an example of using this API using the OSS curl command. In the example below, line breaks and indents have been added for clarity. There are no line breaks or indentation in the actual output. Also, the output order of JSON properties is undefined.

```
>curl --request GET "http://localhost:20714/api/v2/silences"
[
    {
        "id": "787594fd-29a6-495d-921a-d37709f6186e",
        "status": {
            "state": "pending"
        },
        "updatedAt": "2021-08-07T02:02:56.206Z",
        "comment": "cpu alert silence",
        "createdBy": "api",
        "endsAt": "2021-08-15T05:00:00.000Z",
        "matchers": [
            {
                "isEqual": true,
                "isRegex": false,
                "name": "alertname",
                "value": "cpu alert"
            }
        ],
        "startsAt": "2021-08-15T04:00:00.000Z"
    }
]
>
```

5.21.4 Silence creation of Alertmanager

Description

Pass the JSON format silence settings as arguments and create a silence in Alertmanager.

The silence ID returned as a response is an identifier uniquely assigned to the silence setting. Used to run Alertmanager's silence revocation API.

When you set silence, Alertmanager automatically adds the following:

- id
- status
- status.state
- updatedAt
- matchers.isEqual

Format

Request line

```
POST /api/v2/silences HTTP/1.1
```

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*`:`*Port number* "`:`*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.
Content-Type	Specify the format of the request headers as follows: `Content-Type: application/json` This header is optional.

Request message body

```
{
    "matchers": [
        {
            "name": "label name",
            "value": "value",
            "isRegex": Regular expression flags
        },
        ...
    ],
    "startsAt": "Start date and time",
    "endsAt": "End date and time",
    "createdBy": "Author Name",
    "comment": "comment",
}
```

Request parameters

Member name		Data type	Description
matchers		object	An object that specifies the conditions under which alerts are suppressed. Suppresses the issuance of alerts that match the label name and label value specified by name and value.
	name	string	Specify a label name. You can specify the following values for the label name: • Metric label name • Label name (e.g. jp1_pc_eventid) set under labels in the alert configuration file (jpc_alerting_rules.yml) • "alertname" label# Note # To suppress the issuance of alerts based on the alert name, specify "alertname" in the name member and the alert name in the value member. Only single-byte alphanumeric characters can be specified. You cannot specify an empty string.
	value	string	Specify a value for the label. You cannot specify an empty string.
	isRegex	boolean	Specifies whether the value of value is specified as a regular expression. • true

Member name		Data type	Description
			It is specified by a regular expression. • false Not specified in a regular expression.
startsAt		string	Specify the date and time when silence can be applied (ISO8601 extended format). You can specify a time zone for the date and time. (Designated example)2022-02-08T19:00:00+09:00
endsAt		string	Specify the date and time when silence is applied (ISO8601 extended format). If you specify a date and time earlier than startAt or an expired date and time (a date and time earlier than the current time), silence creation fails. You can specify a time zone for the date and time. (Designated example)2022-02-08T21:00:00+09:00
createdBy		string	Specifies the author name.
comment		string	Specify a comment.

Response message body

```
{
"silenceID":"silenceID"
}
```

Status codes

Status code	Message	Description
200	OK	Silence was successfully created.
Other than 200	Other than OK	Silence creation failed.

Examples

The following is an example of using this API using the OSS curl command.

```
> curl --header "Content-Type: application/json" --request POST --data @C:
\tmp\silence.json "http://localhost:20714/api/v2/silences"
{"silenceID":"9ae46d02-4db8-4098-a8e4-f9181d66611c"}
>
```

silence.json:

```
{
    "matchers": [
        {
            "name": "alertname",
            "value": "cpu idel alert",
            "isRegex": false
        }
    ],
    "startsAt": "2021-08-09T19:00:00+09:00",
    "endsAt": "2021-08-09T21:00:00+09:00",
    "createdBy": "api",
    "comment": "test silence"
}
```

5.21.5 Silence Revocation of Alertmanager

Description

Revokes (expires) silences created in Alertmanager.

Format

Request line

```
DELETE /api/v2/silence/silenceID HTTP/1.1
```

The silence ID can be a value to be retrieved by the "Get Alertmanager Silence List" API or a value returned as a return value of the "Create Alertmanager Silence" API.

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*:*Port number* ":*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Response message body

None

Status codes

Status code	Message	Description
200	OK	Silence has successfully expired.
Other than 200	Other than OK	Silence failed to expire.

Examples

The following is an example of using this API using the OSS curl command.

```
>curl --request DELETE "http://localhost:20714/api/v2/silence/b37a053b-617
2-46dd-8211-be808cc25e01"

>
```

5.21.6 Get silence of Alertmanager

Description

Gets the specified silence in JSON format.

Format

Request line

```
GET /api/v2/silence/silence ID HTTP/1.1
```

For *silence ID*, you can specify value to be returned as the return value of value and silence creation for Alertmanager API to be retrieved in silence list retrieval API of Alertmanager.

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*:*Port number* ":*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Response message body

```
{
    "id": "silence ID",
    "status": {
        "state": "Status"
    },
    "updatedAt": "Update Date/time",
    "comment": "Comment",
    "createdBy": "Author-name",
    "endsAt": "Exit Date/time",
    "matchers": [
        {
            "isRegex":Regex flag,
            "name": "Label name",
            "value": "Value"
        },
        ...
    ],
    "startsAt": "Starting Date/time"
}
```

Response parameters

See *Response parameters* in the *5.21.3 Get silence list of Alertmanager*.

Status codes

Status code	Message	Description
200	OK	Silence was successfully acquired.
Other than 200	Other than OK	Failed to get silence.

Examples

The following is an example of how this API can be used with execution using curl command of OSS. In the use cases below, line breaks and indentation are added for clarity. Newlines and indents are not printed in the actual output. The order of JSON properties is undefined.

```
> curl --request GET "http://localhost:20714/api/v2/silence/00ed3d4d-da1f
-4971-81cd-b2687933e602"
{
    "id":"00ed3d4d-da1f-4971-81cd-b2687933e602",
    "status":{
        "state":"active"
    },
    "updatedAt":"2022-08-09T03:35:41.821Z",
    "comment":"cc",
    "createdBy":"aa",
    "endsAt":"2022-08-09T05:35:32.825Z",
    "matchers":[
        {
            "isEqual":true,
            "isRegex":false,
            "name":"env",
            "value":"production"
        }
    ],
    "startsAt":"2022-08-09T03:35:41.821Z"
}
```

5.22 API for Blackbox exporter operation

Describes operations related to Blackbox exporter operation-related API.

5.22.1 Reload Blackbox exporter

Description

Reloads the Blackbox exporter definition file and reflects the operation of the Blackbox exporter.

Reloading the Blackbox exporter is faster than restarting the Blackbox exporter and maintains the state it was in when the notification failed.

Format

Request line

```
POST /-/reload HTTP/1.1
```

Request header

Header name	Setup values
Host	Specifies value of the header for Alertmanager host to which API is connected, in the following format: *Host name* or *IP address*`:`*Port number* "`:`*Port number*" is optional. • *Host name* or *IP address* Specifies host name or IPv4 address of Alertmanager. • *Port number* Specifies port number to use when connecting to Alertmanager. This header is not optional.

Request message body

None

Response message body

If the reload is successful, there is no response.

If the reload fails, a message (the value printed by the Blackbox exporter) is set indicating the cause of the failure.

Status codes

Status code	Message	Description
200	OK	Reloaded successfully.
Other than 200	Other than OK	Reload failed.

Notes

- If you reload an invalid definition file, all contents of the imported definition file will be invalidated.
- The reload will take effect from the next Blackbox exporter API (such as scrape) and will not affect the running API.

Examples

The following is an example of using this API using the OSS curl command.

On successful reload:

```
>curl --request POST "http://localhost:20715/-/reload"

>
```

On reload failure:

```
# curl -request POST http://localhost:20715/-/reload
failed to reload config: error parsing config file: yaml: unmarshal error
s:
  line 3: field priber not found in type config.plain
```

5.23 API for scrape of Exporter used by JP1/IM - Agent

Description

Scrape each exporter that you want to scrape on the Prometheus server. Scrape is performed at the interval set in item "scrape_interval" of the Prometheus configuration file (jpc_prometheus_server.yml).

Even if a status code other than 200 is returned, it will not be retried.

Communication method

Communication protocol: HTTP

Port number: Exporter's port number

Format

Request line

```
GET /metrics# HTTP/1.1
```

The only communication protocol is "HTTP". Specifies the port number of the exporter.

#

The "/metrics" part can be changed in item "metrics_path" of [scrape_configs] of the Prometheus configuration file (jpc_prometheus_server.yml).

Request header

Header name	Setup values
host	The value of the item "targets" in the Prometheus configuration file (jpc_prometheus_server.yml) is set.
user-agent	Prometheus/2.23.0 is set.
accept	"application/openmetrics-text; version=0.0.1,text/plain;version=0.0.4;q=0.5,*/*;q=0.1" is set.
accept-encoding	"gzip" is set.
x-prometheus-scrape-timeout-seconds	The value of the item "scrape_timeout" in the Prometheus configuration file (jpc_prometheus_server.yml) is set.
Other	Authentication information is added according to the settings of the Prometheus configuration file (jpc_prometheus_server.yml).

Request message body

None

Response message body

Returns information in the Prometheus text format shown below.

■Basic Information

Items	Description
Supported Prometheus versions	0.40 or later
Communication protocol	HTTP
Encoding	UTF-8 Use the newline character "\n".
HTTP Content Data Format (Content-Type)	text/plain; version=0.0.4 If there is no version value, it is treated as the latest text format version.
HTTP Content Encoding (Optional) -	gzip

Items	Description
Supported metrics	• Counter • Gauge • Histogram • Summary • Untyped

■Text formatting details

- Written line-by-line.
- The newline character at the end of a line must be '\n'.
- Empty lines are ignored.

■Row formatting

- Tokens on a single line can be separated by any number of spaces or tabs.
- Leading and trailing whitespace is ignored.

■Comments,Help Text,Type Information

- Lines beginning with "#" are treated as comments. Lines where the token immediately after the "#" is not "HELP" or type information are ignored.
- If the token immediately following the "#" is "HELP", at least one token with the metric name is required. All remaining tokens are considered descriptive for that metric name.

  Lines of help text can contain any UTF-8 string after the metric name, but backslashes (\) and newline characters (\n) must be escaped, such as "\\" and "\\n".

  Only one line of help text can be written per metric name.
- If the token immediately following the "#" is type information, describe two or more tokens. The first is the metric name, and the second is counter, gauge, histogram, summary, or untyped, which defines the type of metric.

  Only one line of type information can be described per metric name.

  A row of type information must appear before the first sample for the metric name on that row.

  If no line of type information exists for a metric name, the type of the metric is set to "untyped".

■Sample syntax

```
metric_name [
    "{" label_name "=" `"` label_value `"` { "," label_name "=" `"` lab
el_value `"` } [ "," ] "}"
] value [ timestamp ]
```

- metric_name and label_name have the limitations of normal Prometheus writing.
- label_value can be any UTF-8 string. Backslashes (\), double quotes ("), and line feeds must be escaped as "\\", "\"", and "\\n", respectively.
- value is a floating-point number required by Go's ParseFloat() function. In addition to regular numbers, NaN (not numeric), +Inf (positive infinity), and -Inf (negative infinity) values are also valid.
- The timestamp is int64 (milliseconds (excluding leap seconds) since 1970-01-01 00:00:00 UTC). It is displayed as needed in Go's ParseInt() function.

■Grouping and sorting

- All rows for a metric must be provided as a group, along with an optional help text line and a line of type information.

- Each row must be a unique combination of metric name and label.

■Examples of text formatting

```
# HELP http_requests_total The total number of HTTP requests.
# TYPE http_requests_total counter
http_requests_total{method="post",code="200"} 1027 1395066363000
http_requests_total{method="post",code="400"}    3 1395066363000

# Escaping in label values:
msdos_file_access_time_seconds{path="C:\\DIR\\FILE.TXT",error="Cannot f
ind file:\n\"FILE.TXT\""} 1.458255915e9

# Minimalistic line:
metric_without_timestamp_and_labels 12.47

# A weird metric from before the epoch:
something_weird{problem="division by zero"} +Inf -3982045

# A histogram, which has a pretty complex representation in the text fo
rmat:
# HELP http_request_duration_seconds A histogram of the request duratio
n.
# TYPE http_request_duration_seconds histogram
http_request_duration_seconds_bucket{le="0.05"} 24054
http_request_duration_seconds_bucket{le="0.1"} 33444
http_request_duration_seconds_bucket{le="0.2"} 100392
http_request_duration_seconds_bucket{le="0.5"} 129389
http_request_duration_seconds_bucket{le="1"} 133988
http_request_duration_seconds_bucket{le="+Inf"} 144320
http_request_duration_seconds_sum 53423
http_request_duration_seconds_count 144320

# Finally a summary, which has a complex representation, too:
# HELP rpc_duration_seconds A summary of the RPC duration in seconds.
# TYPE rpc_duration_seconds summary
rpc_duration_seconds{quantile="0.01"} 3102
rpc_duration_seconds{quantile="0.05"} 3272
rpc_duration_seconds{quantile="0.5"} 4773
rpc_duration_seconds{quantile="0.9"} 9001
rpc_duration_seconds{quantile="0.99"} 76656
rpc_duration_seconds_sum 1.7560473e+07
rpc_duration_seconds_count 2693
```

6 Customization of Integrated Operation Viewer Window

This chapter describes the functionality for displaying a window that the user defined in the Related information area when selecting a specific IM management node in the Integrated Operation Viewer window of JP1/IM - Manager (Intelligent Integrated Management Base).

6.1 Overview of Integrated Operation Viewer Window customization

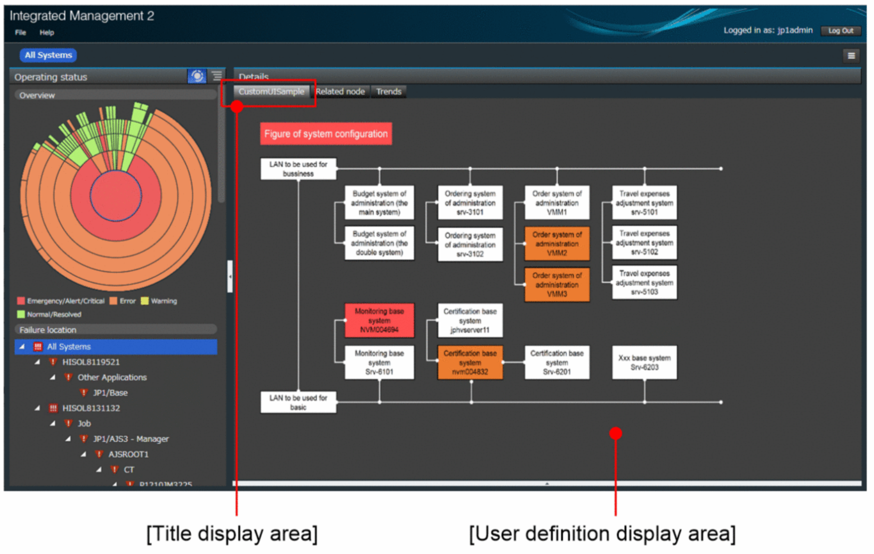
This section describes the overview of customization of the Integrated Operation Viewer window and the location of definition files.

6.1.1 What is customization of the Integrated Operation Viewer window?

In the customization of the Integrated Operation Viewer window, when the user has selected a certain IM management node, all windows that are based on the information determined in advance can be shown in **Custom UI** tab of the Related information area. In addition, you can also define the titles of the areas.

The following figure shows a window image of the applied customization of the Integrated Operation Viewer window.

Figure 6–1: Example of applying customization to the Integrated Operation Viewer window


Integrated Management 2
File
Help
Logged in as: jp1admin
Log Out
All Systems
Operating status
Overview
Emergency/Alert/Critical
Error
Warning
Normal/Resolved
Failure location
All Systems
HISOL8119521
Other Applications
JP1/Base
HISOL8131132
Job
JP1/AJS3 - Manager
AJSROOT1
CT
Details
CustomUISample
Related node
Trends
Figure of system configuration
LAN to be used for bussiness
Budget system of administration (the main system)
Budget system of administration (the double system)
Ordering system of administration srv-3101
Ordering system of administration srv-3102
Order system of administration VMM1
Order system of administration VMM2
Order system of administration VMM3
Travel expenses adjustment system srv-5101
Travel expenses adjustment system srv-5102
Travel expenses adjustment system srv-5103
Monitoring base system NVM004694
Monitoring base system Srv-6101
Certification base system jphvserver11
Certification base system nvm004832
Certification base system Srv-6201
Xxx base system Srv-6203
LAN to be used for basic

[Title display area]

[User definition display area]

6.1.2 The storage location

Place the customization definition file of the Integrated Operation Viewer window in the HTML format in the following location by creating a sub folder or subdirectory. Physical hosts and logical hosts are placed in the same location. In a cluster configuration, place the same file in both systems.

Note that subdirectory names starting with `hitachi` cannot be used.

In Windows:

Manager-path\ `public\customUI\`

In UNIX:

`/var/opt/jp1imm/`public/customUI/

When you uninstall the JP1/IM - Manager, backup files which you located as needed.

6.1.3 Notes

The `<iframe>` tag is used in the custom UI tab. Due to this, if you try to display a Web page by using a property such as `window.location.href` when `X-Frame-Options` is specified for that Web page, you will not be able to display the Web page.

In this case, action is needed on the part of the website providing the Web page to allow access from JP1/IM.

Example of a specification

```
X-Frame-Options ALLOW-FROM <URL-of-JP1/IM>
```

6.2 Customization definition information of the Integrated Operation Viewer window

This section describes the customization definition information of the Integrated Operation Viewer window.

6.2.1 Property information to be defined

The following table shows the property information to be defined.

An item must be specified to a single *custom-UI-Id* in the property. For characters to be specified in *custom-UI-Id*, see *6.2.2 Character string to be specified to custom-UI-Id*.

Table 6–1: Definition information of the customization of the Integrated Operation Viewer window

No.	property name	Required/Optional	Description	Specification range
1	`jp1.imdd.gui.settings.contentViews.`*custom UI Id*`.title`	Required	Specify a title to be displayed in the **Custom UI** tab.[#1] If you specify a long string with half-width alphanumeric characters for the title, the WWW browser can truncate the string displayed as a tooltip for the title of the **Custom UI** tab. When you use half-width space or full-width characters as appropriate in the title string, all the characters are displayed as the tooltip without truncation.	Between 1 and 255 characters
2	`jp1.imdd.gui.settings.contentViews.`*custom UI Id*`.url`	Required	Specify the absolute path from `public` to the HTML file that you want to display in the user definition window display area.[#1] You need to use a forward slash (/) as the path separator character. Even if the path contains a half-width space	Between 1 and 255 characters

No.	property name	Required/Optional	Description	Specification range
			character ( ), you do not have to enclose it with double quotation marks (""). Note that if a path that does not exist is specified to url, the user definition window display area displays a message in the "Not Found *specified-path*" format.	
3	`jp1.imdd.gui.settings.contentViews.`*custom UI Id*`.sid`	Required[#2]	Specify the tree SID of the IM management node for displaying the user definition window. You can use a regular expression[#3] to specify it. Note that whether the specified tree SID exists is not checked.	Between 1 and 1,048,576 characters
4	`jp1.imdd.gui.settings.contentViews.`*custom UI Id*`.target`	Required[#2]	Specify the SID of an IM management node for displaying the user definition window. You can use a regular expression[#3] to specify it. Note that whether the specified SID exists is not checked.	

#1:

For specifying 2-byte characters, convert them to Unicode. In this case, the number of characters is counted as the number of those that have already been converted into Unicode characters. You can specify characters other than control characters. Platform-dependent characters cannot be specified.

#2:

For each *custom-UI-Id*, always specify either `sid or target`. The specifiable characters depend on the specified tree SID or configuration information SID.

#3:

If you use a regular expression, using many "`.*`", which is an expression that matches with all characters, might cause research to take longer. For using "`.*`", keep in mind to use "`.*`" only where necessary.

6.2.2 Character string to be specified to *custom-UI-Id*

You need to specify a character string to *custom-UI-Id* in a property so that the key is unique.

You can specify a character string of half-width alphanumeric characters (case sensitive). Specify 1 to 255 characters. If you define multiple character strings to the same key, the last character that was defined becomes valid. A string starting with `_HITACHI` cannot be specified.

The following shows a specification example:

```
jp1.imdd.gui.settings.contentViews.sample.title =Custom+UI
jp1.imdd.gui.settings.contentViews.sample.url =./customUI/sample/index.html
jp1.imdd.gui.settings.contentViews.sample.target =^(?=.*MYHOST).*$

jp1.imdd.gui.settings.contentViews.sample2.title =Custom+UI
jp1.imdd.gui.settings.contentViews.sample2.url =./customUI/sample2/index.ht
ml
jp1.imdd.gui.settings.contentViews.sample2.sid = _ROOT_AllSystems
```

6.2.3 Description example of the Intelligent Integrated Management Base definition file (imdd.properties)

The definition details are written in the Intelligent Integrated Management Base definition file (`imdd.properties`). See *Intelligent Integrated Management Base definition file (imdd.properties)* in *Chapter 2. Definition Files*.

The following shows the description in the model file (imdd.properties.model) of the Intelligent Integrated Management Base definition file (imdd.properties):

```
server.port = 20703

#jp1.imdd.gui.settings.contentViews.custom UI Id.title =
#jp1.imdd.gui.settings.contentViews.custom UI Id.url =
#jp1.imdd.gui.settings.contentViews.custom UI Id.sid =
#jp1.imdd.gui.settings.contentViews.custom UI Id.target =
```

(1) When multiple custom UIs are displayed

If you define several different `<custom UI Id>` tags for a single IM management node, the **Custom UI** tabs are displayed as many as the number of defined tags.

Note that the **Custom UI** tabs are displayed in the order of the definition in the Intelligent Integrated Management Base definition file (`imdd.properties`).

The following shows a definition example:

```
jp1.imdd.gui.settings.contentViews.System01CustomUI1.title = System01\u30ab\
u30b9\u30bf\u30e0UI1
jp1.imdd.gui.settings.contentViews.System01CustomUI1.url = ./customUI/sample
/customUI1.html
jp1.imdd.gui.settings.contentViews.System01CustomUI1.sid = _ROOT_AllSystems/
_SYSTEM_SYSTEM01
```

```
jp1.imdd.gui.settings.contentViews.System01CustomUI2.title = System01\u30ab\
u30b9\u30bf\u30e0UI2
jp1.imdd.gui.settings.contentViews.System01CustomUI2.url = ./customUI/sample
/customUI2.html
jp1.imdd.gui.settings.contentViews.System01CustomUI2.sid = _ROOT_AllSystems/
_SYSTEM_SYSTEM01

jp1.imdd.gui.settings.contentViews.System01CustomUI3.title = System01\u30ab\
u30b9\u30bf\u30e0UI3
jp1.imdd.gui.settings.contentViews.System01CustomUI3.url = ./customUI/sample
/customUI3.html
jp1.imdd.gui.settings.contentViews.System01CustomUI3.sid = _ROOT_AllSystems/
_SYSTEM_SYSTEM01
```

Important

- The maximum number of **Custom UI** tabs you can display for a single IM management node is 10.

6.2.4 Confirmation of the definition information

To check whether the setting for displaying a desired window when selecting an IM management node was written in the Intelligent Integrated Management Base definition file (`imdd.properties`), see the **Integrated Operation Viewer** window.

Select a target IM management node and check whether the intended window appears. If the definition information is incorrect, check the error details displayed on the console of the Web browser, and then take action.

6.3 Methods and objects that can be used in the user definition window

Load the following `js` files to use the interface provided by the Intelligent Integrated Management Base in html files for user-defined windows.

In Windows

Manager-path`\public\assets\js\customContent.js`

Manager-path`\public\assets\js\vendor.js`

In UNIX

```
/opt/jp1imm/public/assets/js/customContent.js
/opt/jp1imm/public/assets/js/vendor.js
```

For an example of how to use these files, see the usage example in *6.3.1 CustomContent.initialize*.

The following table shows the methods and objects that can be used in the user definition window.

Table 6–2: Methods and objects that can be used in the user definition window

Method name	Functionality
CustomContent.initialize	The method to execute the initialization processing by using the event handler received by the argument.
CustomContent.simt	Provides methods that manipulate the Simt data.
CustomContent.node	The object that has the information on the IM management node that was selected in the integrated operation viewer.
CustomContent.options.props	The object that has the information on the client.
CustomContent.postActions	The method to execute the specified plug-in functions.
CustomContent.showMessage	The method to define a message to be displayed in the title and message display area.
CustomContent.selectNodeByTreeSid	The method to make the IM management node with the SID, which was specified in the argument, selected in the integrated operation viewer.
CustomContent.selectNodeByTargetSid	

6.3.1 CustomContent.initialize

Functionality

This method executes the initialization processing by using the event handler received by the argument.

To draw the user definition window, always execute this method.

Format

```
initialize(handlers)
```

Argument

Defines the events to be obtained in the user definition window and transfers the names of functions to be executed when the events are obtained.

`handlers`

Event handlers

There are the following types of event handlers:

- `onSetup()`

  The setup event handler

  This event handler handles events that occur when the user definition window is drawn for the first time.

- `onActivate()`

  The activation event handler

  This event handler handles events that occur when the drawing of the user definition window is completed.

- `onInactivate()`

  The inactivation event handler

  This event handler handles events that occur when another window is displayed in the drawn user definition window.

- `onNodeSelect(node)`

  The node selection event handler

  This event handler handles events that occur when an IM management node is selected.

- `onStatusUpdate(node)`

  The node status update event handler

  This event handler handles events that occur when the status of the IM management node is updated regardless of the selected IM management node.

Return value

None

Use example

The following are some example cases:

1. When the onSetup event is received, the Setup function of the user definition window is run.
2. When the onNodeSelect event is received, the NodeSelect function of the user definition window is run.
3. When the onActivate event is received, the Activate function of the user definition window is run.

```
<html>
<script src="/assets/js/vendor.js"></script>
<script src="/assets/js/customContent.js"></script>
<script>

CustomContent.initialize({
  onSetup: Setup,
  onNodeSelect: NodeSelect,
  onActivate: Activate
});
function Activate() {
alert("onActivate");
}
function NodeSelect () {
alert("onNodeSelect ");
}
function Setup () {
alert("onSetup");
}
</script>
</html>
```

6.3.2 CustomContent.simt

Provides methods that manipulate the Simt data; the following table shows the methods provided by CustomContent.simt:

Table 6–3: List of methods provided by CustomContent.simt

No.	Method name	Description
1	encodeValue	The method to URL-encode and return a character string.
2	decodeValue	The method to URL-decode a URL-encoded character string and return the character string.
3	filter	The method to return an SID that contains a specified structured identifier as well as its value value.
4	get	The method to return an SID that matches a specified structured identifier as well as its value value.
5	pack	The method to join the class and name of a structured identifier and to return the generated structured identifier.
6	packHost	The method to join the class and host name of a structured identifier and return the generated structured identifier.
7	unpack	The method to split the structured identifier into classes and names and to return them.
8	join	The method to join structured identifiers and return the generated structured identifier.
9	split	The method to split the SID into structured identifiers and return them.
10	parse	The method to split the SID into structured identifiers, further split the split structured identifiers into classes and URL-decoded names, and then to return the classes and the URL-decoded names.
11	data	The method to generate an object from an SID and value value and to return the object.

(1) encodeValue method

Functionality

The method to URL-encode and return symbols other than `.`, ~, `-`, and `:`, and non-alphanumeric characters in the string specified by the parameter.

Format

```
encodeValue(value)
```

Argument

`value`

The character string to be URL-encoded

Return value

The URL-encoded character string

(2) decodeValue method

Functionality

This method decodes the character string specified in the parameter and then returns the character string.

Format

```
decodeValue(value)
```

Argument

`value`

The URL-encoded character string

Return value

The URL-decoded character string

(3) filter method

Functionality

This method generates, from the array of SimtData objects (objects that summarize SIDs and value information) specified for the first parameter, a SimtData object whose SID includes the structured ID specified for the second parameter, and returns that generated SimtData object.

Format

`filter(array, pattern)`

Argument

`array`

The array of the SimtData object#

`pattern`

The structured identifier

Return value

The array of the SimtData object#

The SimtData# that has an SID that contains a structured identifier

If no object exists, an empty array is returned.

#: The SimtData object contains the following properties.

- `sid`: The character string that indicates an SID
- `value`: The object that stores the value of the SID

(4) get method

Functionality

This method generates, from the array of SimtData objects (objects that summarize SIDs and value information) specified for the first parameter, a SimtData object whose SID matches the SID specified for the second parameter, and returns that generated SimtData object.

Format

`get(array, sid)`

Argument

`array`

The array of the SimtData object#

`pattern`

SID

Return value

The SimtData object#

This SimtData# object has an SID that matches the specified SID.

If no object exists, an empty null is returned.

#: The SimtData object contains the following properties.

- `sid`: The character string that indicates an SID
- `value`: The object that stores the value of the SID

(5) pack method

Functionality

This method encloses classes (without underscores) of the structured identifier specified by the first parameter with underscores (_), URL-encodes symbols other than `.`, ~, `-`, and `:`, and non-alphanumeric characters in the name specified by the second parameter, joins the class and the name in this order, and then returns the generated structured identifier.

Format

```
pack(key, value)
```

Argument

`key`

The structured identifier class

`value`

The name of the structured identifier

Return value

The character string of the structured identifier

(6) packHost method

Functionality

This method encloses classes (without underscores) of the structured identifier specified by the first parameter with underscores (_), URL-encodes symbols other than `.`, ~, `-`, and `:`, and non-alphanumeric characters in the name (host name) specified by the second parameter, joins the class and the name in this order, and then returns the generated structured identifier.

If you create a structured identifier with a name other than a host name, use the `CustomContent.simt.pack` method.

Format

```
packHost(key, value)
```

Argument

`key`

The structured identifier class

`value`

The name of the structured identifier (host)

Return value

The character string of the structured identifier

(7) unpack method

Functionality

This method splits the specified structured identifier into classes (without underscores) and URL-decoded names, and then returns the SimtIdUnit object that stores both.

Format

```
unpack(simtId)
```

Argument

`simtId`

The structured identifier

Return value

The SimtIdUnit object#

#: The SimtIdUnit object contains the following properties.

- `key`: The class of a structured identifier (without underscores)
- `value`: The URL-decoded name of a structured identifier

(8) join method

Functionality

This method joins multiple structured identifiers, which are specified in the parameter, with a forward slash (/), and then returns the generated SID.

Format

```
join(...simtId)
```

Argument

`simtId`

The structured identifier.

Return value

The character string of the SID

(9) split method

Functionality

This method splits the SID, which is specified to the parameter, with a forward slash (/), and then returns the structured identifiers.

Format

```
split(sid)
```

Argument

`sid`

SID

Return value

The array of the character string of the structured identifier.

(10) parse method

Functionality

The method to store information (the SID, which is specified to the parameter, is split into structured identifiers, and the split structured identifiers are further split into classes and URL-decoded names from which underscores are eliminated) as a SimtIdUnit object, and then to return the array of stored SimtIdUnit object.

Format

```
parse(sid)
```

Argument

`sid`

SID

Return value

The array of the SimtIdUnit object[#]

#: The SimtIdUnit object contains the following properties.

- `key`: The class of a structured identifier (without underscores)
- `value`: The URL-decoded name of a structured identifier

(11) data method

Functionality

This method generates and returns a SimtData object from the SID and the value value that are specified for the parameters.

Format

```
data(sid, value)
```

Argument

`sid`

SID

`value`

The value value

Return value

The SimtData object[#] that put together the information of the SID and the value value

#: The SimtData object contains the following properties.

- `sid`: The character string that indicates an SID
- `value`: The object that stores the value value of the SID

6.3.3 CustomContent.node

This object has the information on the IM management node that was selected in the integrated operation viewer. The following table shows the properties of CustomContent.node.

Table 6–4: CustomContent.node properties

No.	Property name	Description
1	CustomContent.node.sid	The tree SID information of the IM management node that was selected in the integrated operation viewer.
2	CustomContent.node.value.target	The SID information of the IM management node that was selected in the integrated operation viewer.
3	CustomContent.node.value.label	The label information of the IM management node that was selected in the integrated operation viewer.

6.3.4 CustomContent.options.props

The object that has the information on the client. The following shows the CustomContent.options.props properties.

Table 6–5: CustomContent.options.props properties

No.	Property name	Description
1	CustomContent.options.language	Information on the language class of the client
2	CustomContent.options.clientId	Client ID information
3	CustomContent.options.props.title#	Setting information of title associated with the IM management node that was selected in the integrated operation viewer
4	CustomContent.options.props.url#	Setting information of url associated with the IM management node that was selected in the integrated operation viewer
5	CustomContent.options.props.target#	Setting information of target associated with the IM management node that was selected in the integrated operation viewer
6	CustomContent.options.props.sid#	Setting information of sid associated with the IM management node that was selected in the integrated operation viewer
7	CustomContent.options.auth.jp1user	Information on the logged-in JP1 user ID
8	CustomContent.options.auth.jp1token	Information on the JP1 token of the logged-in JP1 user
9	CustomContent.options.auth.token	Information on the token of the client
10	CustomContent.options.auth.acl.permissions	Array of the permissions of the logged-in JP1 user

#

The values defined for the following parameters in the Intelligent Integrated Management Base definition file (`imdd.properties`) are displayed.

Property of the CustomContent.options.props	Parameters of the imdd.properties
CustomContent.options.props.title	jp1.imdd.gui.settings.contentViews.<custom UI Id>.title
CustomContent.options.props.url	jp1.imdd.gui.settings.contentViews.<custom UI Id>.url
CustomContent.options.props.target	jp1.imdd.gui.settings.contentViews.<custom UI Id>.target
CustomContent.options.props.sid	jp1.imdd.gui.settings.contentViews.<custom UI Id>.sid

6.3.5 CustomContent.postActions

Functionality

This method runs functions of the specified plug-in.

Format

```
postActions(method, sid, args)
```

Argument

`method`

The name of the plug-in to be run

`sid`

The SID of the IM management node that is subject to plug-in processing

`args`

Specifies the value to be passed to the argument args.methodArgs of the plug-in functions to be executed. If no information is to be passed, an empty object ({}) is specified.

Return value

This object shows the result of the executed action. The content of the object varies depending on the executed action.

6.3.6 CustomContent.showMessage

Functionality

This method displays the character string specified for the message argument in the message display area.

When the specified character string starts with the message ID of an error, ❗ is displayed before the message.

When the specified character string starts with the message ID of a warning, ⚠ is displayed before the message.

In other cases, ℹ is displayed before the message.

Format

```
showMessage(message)
```

Argument

`message`

The character string to be displayed in the message display area

Return value

None

6.3.7 CustomContent.selectNodeByTreeSid

Functionality

This method selects, in the integrated operation viewer, the IM management node with the tree SID, which was specified in the argument.

Format

selectNodeByTreeSid(sid)

Argument

`sid`

The tree SID of the IM management node to be selected in the integrated operation viewer

Return value

None

6.3.8 CustomContent.selectNodeByTargetSid

Functionality

This method selects, in the integrated operation viewer, the IM management node with the SID, which was specified in the argument.

Format

```
selectNodeByTargetSid(sid)
```

Argument

`sid`

The tree SID of the IM management node to be selected in the integrated operation viewer

Return value

None

7 Information Necessary to Use the Intelligent Integrated Management Base

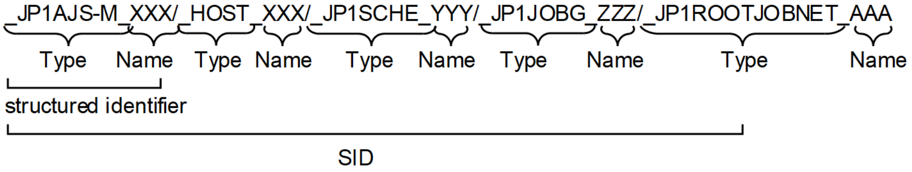
This chapter describes the SIDs and json objects that are necessary to use the Intelligent Integrated Management Base, the adapter command information that is necessary to use user-created plug-ins, and the functionality provided to generate an IM management node tree. It also provides a sample plug-in and details regarding the control characters.

7.1 SID

A SID is an identifier that uniquely identifies components of each product retrieved using the configuration collection adapter command and a user-created plug-in. There are three types of SIDs: configuration information SIDs, tree SIDs, and event SIDs. SIDs are assigned by JP1/IM - Manager (Intelligent Integrated Management Base).

A unique SID is composed of class-name pairs, each of which is separated by a forward slash (/). A pair (structured identifier) is a combination of the class of a component element and the name of the component element in the class. The following example illustrates the structure of a SID.

Figure 7–1: Example illustrating the structure of a SID


_JP1AJS-M_XXX/_HOST_XXX/_JP1SCHE_YYY/_JP1JOBG_ZZZ/_JP1ROOTJOBNET_AAA
Type
Name
Type
Name
Type
Name
Type
Name
Type
Name
structured identifier
SID

The order of pairs is not arbitrary, which represents nested component elements in the product. For details, see the section that describes the information retrieved from each product in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*.

The following rules govern SIDs:

- The class and name of the SID can accept ASCII characters, except for the three types of characters of underscore (_), forward slash (/), and control codes.
- URL-encode any symbols other than the period (.), tilde (~), hyphen (-) and corron (:) as well as any non-alphanumeric characters. A URL-encoded SID must be URL-decoded.
- A host name must be specified in uppercase letters. Letters in a SID are case sensitive.
- The byte length of the SID ranges from 1 to 1,048,576 bytes (1 MB). The SID must not end with a forward slash (/).

7.1.1 Configuration information SID

A configuration information SID represents system configuration information.

There are different classes to configuration information SIDs, some of which are specific to each product while others are used commonly across products. The following table describes the reserved words for the class names used by the individual configuration information SIDs.

Table 7–1: Reserved words for the class names of configuration information SIDs

No.	Applicable product	Class name[#1]	Description	Name to be specified[#2]
1	Common	_HOST_	Indicates a host.	The name of the host
2	JP1/AJS3	_JP1AJS-M_	Indicates JP1/AJS3 - Manager.	The name of the host running JP1/AJS3 - Manager
3		_JP1AJS-A_	Indicates JP1/AJS3 - Agent.	The name of the host running JP1/AJS3 - Agent

No.	Applicable product	Class name[#1]	Description	Name to be specified[#2]
4		`_JP1AJSMGR_`	Indicates JP1/AJS3 - Manager.	None
5		`_JP1AJSAGT_`	Indicates JP1/AJS3 - Agent.	None
6		`_JP1AJSSCHE_`	Indicates the scheduler service of JP1/AJS3.	None
7		`_JP1ROOTJOBNET_`	Indicates a root jobnet.	The name of the root jobnet
8		`_JP1ROOTJOBNETDUMMY_`	Indicates that the preceding node or succeeding node is unknown in link information of a jobnet.	UNKNOWN
9	JP1/AJS3 JP1/IM	`_JP1SCHE_`	Indicates a scheduler service.	The name of the scheduler service
10		`_JP1JOBG_`	Indicates a job group.	The name of the job group
11	JP1/PFM	`_JP1PFM-M_`	Indicates JP1/PFM - Manager.	The name of the host running JP1/PFM - Manager
12		`_JP1PFM-A_`	Indicates the service ID of JP1/PFM - Agent or JP1/PFM - RM.	Service ID
13		`_JP1PFM-AHOST_`	Indicates the name of the host on which JP1/PFM - Agent or JP1/PFM - RM runs, or the name of a managed host of JP1/PFM - RM.	The name of the host on which JP1/PFM - Agent or JP1/PFM - RM runs, or the name of a managed host of JP1/PFM - RM
14		`_JP1PFMMGR_`	Indicates JP1/PFM - Manager.	None
15		`_JP1PFMBASE_`	Indicates JP1/PFM-Base.	None
16		`_JP1AGENTSERVICE_`	Indicates the service of JP1/PFM - Agent or JP1/PFM - RM.	None
17	JP1/IM JP1/Base	`_JP1IM_`	Indicates that the host is the JP1/IM integrated manager.	The name of the host running the JP1/IM integrated manager
18		`_JP1IMBASEMGR_`	Indicates that the host is an IM base or relay manager.	The name of the host running the IM base or relay manager
19		`_JP1IMRM_`	Indicates that the host is a remotely monitored host.	The name of the remotely monitored host
20		`_JP1IMMGR_`	Indicates JP1/IM - Manager.	None
21		`_JP1BASE_`	Indicates that the host runs JP1/Base.	The name of the host running JP1/Base

No.	Applicable product	Class name[#1]	Description	Name to be specified[#2]
22		`_JP1BASEAGT_`	Indicates JP1/Base.	None
23		`_JP1BASETRAP_`	Indicates a log file trap or event log trap.	None
24	JP1/IM	`_ROOT_`	Indicates the root name of the system.	The root name of the system
25		`_SYSTEM_`	Indicates a system.	The name of the system
26		`_CATEGORY_`	Indicates a category.	The name of the category
27		`_SUBCATEGORY_`	Indicates a subcategory.	The name of the subcategory
28		`_OBJECT_`	Indicates a management object	The name of the management object
29	JP1/NNMi	`_JP1NNMI-M_`	Indicates JP1/NNMi.	The name of the host running JP1/NNMi.
30		`_JP1NNMI-A_`	Indicates a node detected by JP1/NNMi.	The name of the node detected by JP1/NNMi
31		`_JP1NNMiMGR_`	Indicates JP1/NNMi.	None
32		`_NNMINODE_`	Indicates a node detected by JP1/NNMi.	None
33	JP1/OA JP1/NNMi JP1/SSO	`_NETWORKDEVICE_`	Indicates a network device.	Host name, IP switch name, or FC switch name
34	JP1/OA	`_JP1OA`	Indicates JP1/OA.	The name of the host running JP1/OA.
35		`_JP1OA-A`	Indicates a monitoring target of JP1/OA.	The name of the monitoring target of JP1/OA
36		`_JP1OAMGR_`	Indicates JP1/OA.	None
37		`_CONSUMER_`	Indicates a monitoring target (consumer).	The name of the consumer
38		`_CONTAINERCLUSTER_`	Indicates a monitoring target (container cluster).	The name of the container environment cluster
39		`_CONTAINERNODE_`	Indicates a monitoring target (container node).	The name of the container environment node
40		`_SERVERCLUSTER_`	Indicates a monitoring target (cluster).	The name of the cluster
41		`_HYPERVISOR_`	Indicates a monitoring target (hypervisor).	The name of the hypervisor
42		`_VM_`	Indicates a monitoring target (virtual machine).	The name of the virtual machine
43		`_STORAGE_`	Indicates a monitoring target (storage system).	The name of the storage system

No.	Applicable product	Class name#1	Description	Name to be specified#2
44		`_STORAGEVOLUME_`	Indicates a monitoring target (volume).	The name of the volume
45	JP1/SSO	`_JP1SSO-M_`	Indicates that the SID is related to an SSO manager.	The name of the host running JP1/SSO
46		`_JP1SSO-A_`	Indicates that the SID is related to an SSO agent.	The name of the SSO agent host
47		`_JP1SSOMGR_`	Indicates an SSO manager.	None
48		`_JP1SSOAGT_`	Indicates an SSO agent.	None

#1

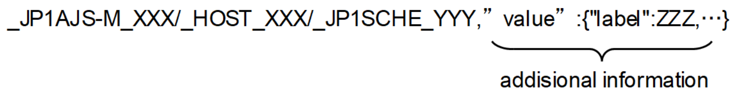
Each class name is 1 to 255 characters long.

#2

Each name must be 0 to 255 characters long, with the exception of the name specified for the object root node class, which must be 1 to 255 characters long.

The configuration information SID has, in addition to the value corresponding to the applicable class, additional information assigned to it in the form of a value specified for `value`. The following figure shows what the additional information looks like.

Figure 7–2: Example of additional information specified in a configuration information SID


_JP1AJS-M_XXX/_HOST_XXX/_JP1SCHE_YYY,” value” :{"label":ZZZ,···}
addisional information

The following table describes the additional information items specified in the configuration information SID.

Table 7–2: Additional information specified in the configuration information SID

No.	Applicable product	Variable name	Description
1	Common	`component`	The component name. It is the `component` value of the `__configurationGet` method. This information is specified in all configuration information SIDs.
2		`jp1ResourceGroup`	Specify a JP1 resource group name from 1 to 64 characters. The permitted characters are half-width alphanumeric characters and the following half-width symbols: !#$%&'()*-.@\^_`{}~ This variable can be omitted.
3		`category`	Specify a category from 1 to 255 characters. The permitted characters are half-width alphanumeric characters. For the acceptable values, see *Table 4-2 Category IDs that the category variable can accept*. This variable can be omitted.
4		`subCategory`	Specify the abbreviated name of a product from 1 to 255 characters. The permitted characters are characters other than control characters. For JP1 products, this information is represented by a string starting with `JP1/`. This variable can be omitted.
5		`visible`	Specify whether to show the component in the **Operating status** area. • `true`: Show • `false`: Do not show Specify `true`.

No.	Applicable product	Variable name	Description
6		label	Specify the display name of a component that is shown in the tree from 1 to 255 characters. The permitted characters are characters other than control characters. For JP1 products, this information is represented by a string starting with JP1/. This variable can be omitted.
7		methods	A list of plug-in functions that can work with the component through the plug-in. This information allows the function to be executed regardless of which product the plug-in belongs to. In order for this to work, it is important that you do not register a product-specific function. Make sure that the name of the function you register starts with an underscore (_). The information for the client to identify whether the plug-in function can work with the node. Considering the scalability of the user plug-in, use return immediately without a plug-in that corresponds to a node causing an error if a method that is not found in methods is invoked.
8		property	Specify property information of each components in object format. The number of elements you can specify ranges from 0 to 100. Property names can accept characters from 1 to 64 characters, other than control characters. Property values can accept characters from 1 to 255 characters, other than control characters. This variable can be omitted. Example: "property":{"DataModelVersion":"yyy",...}
9		jp1im_TrendData_labels	When referencing trend data, specifies the label name and label Value associated with SID in object format. The number of elements that can be specified is 0 to 100. You can specify a property name that is from 1 to 255 control characters. The property Value can be from 1 to 2,595 non-control characters. This variable can be omitted. Example of specification: "jp1im_TrendData_labels":{"instance":"host1:9001"}
10	JP1/AJS	jobExecAgentList	Execution agent name information
11	JP1/PFM	productId	Product ID of JP1/PFM - Agent or JP1/PFM - RM
12		dataModelVersion	Data model version of JP1/PFM - Agent or JP1/PFM - RM
13		wcHostName	Host name of JP1/PFM - Web Console
14		portNumber	Port number of JP1/PFM - Web Console
15		protocol	https communication setting

7.1.2 Tree SID

A tree SID shows a path to a specific node in the system management tree. Specifically, it represents a path to one of the IM management nodes displayed in tree view.

A tree SID consists of the name of the class to which the component in question belongs and the component name relevant to the class (structured identifier), which, when put together with a slash (/), takes the form of a path to the corresponding node.

Unlike the configuration information SID, the tree SID must begin with _ROOT_AllSystems. The maximum number of hierarchies for the entire tree is 45layers.

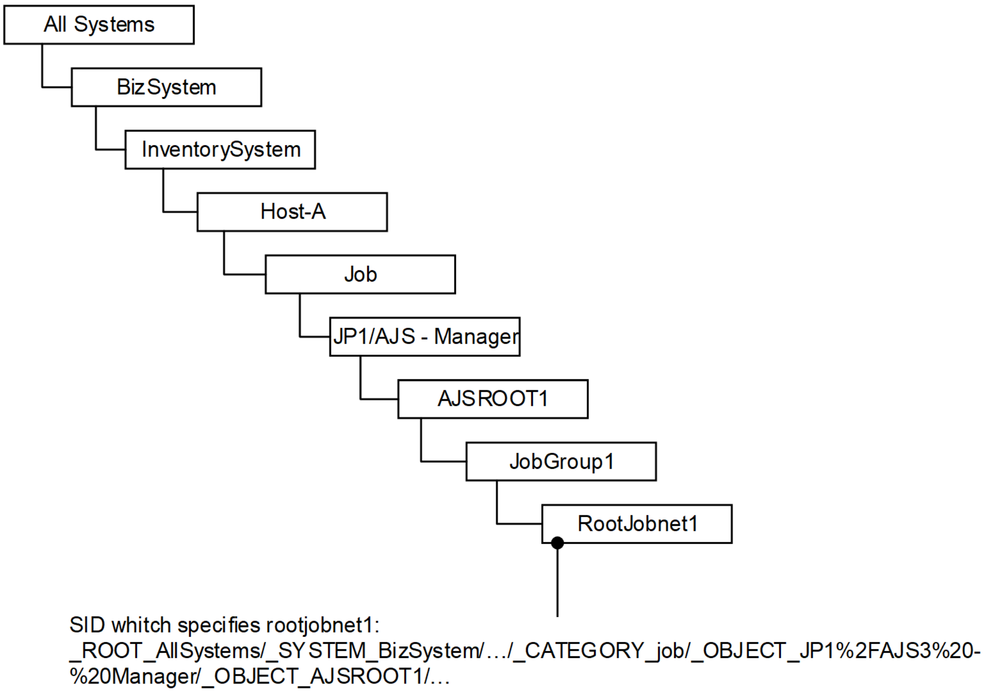
The following table lists classes used in a tree SID.

Table 7–3: Reserved words for the class names of the tree SID

No.	Class name	Description
1	`_ROOT_`	Indicates the root name of the system. Specify the root name of the system for the name.
2	`_SYSTEM_`	Indicates a system. Specify the system name for the name.
3	`_HOST_`	Indicates a host. Specify the host name for the name.
3	`_CATEGORY_`	Indicates a category. Specify the category name for the name.
4	`_SUBCATEGORY_`	Indicates a subcategory. Specify the subcategory name for the name.
5	`_OBJECT_`	Indicates a management object. Specify the management object name for the name.

The following example illustrates the structure of a tree and tree SIDs.

Figure 7–3: Example illustrating the structure of a tree and tree SIDs



SID whitch specifies rootjobnet1:
_ROOT_AllSystems/_SYSTEM_BizSystem/.../_CATEGORY_job/_OBJECT_JP1%2FAJS3%20-%20Manager/_OBJECT_AJSROOT1/...

The following table describes the additional information for the tree.

Table 7–4: Additional information for the tree

Variable name	Description
`target`	The configuration information SID corresponding to the tree SID When there is no configuration information SID corresponding to the tree SID, specify an empty array. The SID you specify must specify the SID that exists.
`label`	The display name of the component to be displayed on the tree It inherits `label` of additional information for the SID or the information of `displayName` in the system node definition file (`imdd_systemnode.conf`). If there is no such information, this variable can be omitted.
`resourceGroup`	The resource group It inherits `label` of additional information for the SID or the information of `jp1ResourceGroup` in the system node definition file (`imdd_systemnode.conf`).

Variable name	Description
	If there is no such information, this variable can be omitted.

For details about the system node definition file (`imdd_systemnode.conf`), see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files*.

7.1.3 JP1 Event SID

A JP1 event SID uniquely identifies each JP1 event.

The following table describes the classes of JP1 event SID.

Table 7–5: Reserved words for the class names of the JP1 event SID

No.	Class name	Description
1	`_JP1IM`	Indicates a JP1IM event. Specify the IM manager host name for the name.
2	`_JP1IMSEQNO_`	Indicates a serial number in the integrated monitoring database. Specify the serial number in the integrated monitoring database for the name.
3	`_JP1IMEVBSEQNO_`	Indicates a serial number in the event database. Specify the serial number in the event database for the name.

Example of the JP1 event SID

```
_JP1IM_imhost1/_JP1IMSEQNO_697/_JP1IMEVBSEQNO_7
```

7.1.4 Information retrieved from each product

Each product that links with JP1/IM - Manager (Intelligent Integrated Management Base) creates an SID from its configuration information retrieved with the adapter command and plug-in. The Intelligent Integrated Management Base manages created SIDs.

This section provides the types and formats of information retrieved from each product. The content of `value` depends on each product.

(1) Information retrieved from JP1/IM or JP1/Base

The following table lists the types and formats of the information retrieved from JP1/IM or JP1/Base.

Table 7–6: Types and formats of the information retrieved from JP1/IM or JP1/Base

Type of information	Format
The name of the host running JP1/IM - Manager (Integrated manager)	`{"sid":"_JP1IM_`*integrated-manager-host-name*`/_HOST_`*integrated-manager-host-name*`","value":{...}},...`
JP1/IM - Manager (Integrated manager) running on the host described above	`{"sid":"_JP1IM_`*integrated-manager-host-name*`/_HOST_`*integrated-manager-host-name*`/_JP1IMMGR_","value":{...}},...`
The host running the integrated manager and JP1/Base under the integrated manager	`{"sid":"_JP1IM_`*integrated-manager-host-name*`/_JP1BASE_`*Base-host-name*`/_HOST_`*Base-host-name*`","value":{...}},...`

Type of information	Format
The integrated manager and JP1/Base under the integrated manager running on the host described above	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1BASE_*Base-host-name*/_HOST_*Base-host-name*/_JP1BASEAGT_","value":{...}},...
Log file traps and event log file traps performed on the host running the integrated manager and JP1/Base under the integrated manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1BASE_*Base-host-name*/_HOST_*Base-host-name*/_JP1BASETRAP_","value":{...}},...
The remotely monitored host under the integrated manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMRM_*remotely-monitored-host-name*/_HOST_*remotely-monitored-host-name*","value":{...}},...
Log file traps and event log file traps performed on the remotely monitored host under the integrated manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMRM_*remotely-monitored-host-name*/_HOST_*remotely-monitored-host-name*/_JP1BASETRAP_","value":{...}},...
The host running the base or relay manager under the integrated manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_HOST_*base-or-relay-manger-host-name*","value":{...}},...
JP1/IM - Manager (base or relay manager under the integrated manager) running on the host described above	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_HOST_*base-or-relay-manager-host-name*/_JP1IMMGR_","value":{...}},...
The host running the base or relay manger and JP1/Base under the base or relay manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_JP1BASE_*Base-host-name*/_HOST_*Base-host-name*","value":{...}},...
The base or relay manger and JP1/Base under the base or relay manager running on the host described above	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_JP1BASE_*Base-host-name*/_HOST_*Base-host-name*/_JP1BASEAGT_","value":{...}},...
Log file traps and event log file traps performed on the host running the base or relay manager and JP1/Base under the base or relay manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_JP1BASE_*Base-host-name*/_HOST_*Base-host-name*/_JP1BASETRAP_","value":{...}},...
The remotely monitored host and the host under the base or relay manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_JP1IMRM_*remotely-monitored-host-name*/_HOST_*remotely-monitored-host-name*","value":{...}},...
Log file traps and event log file traps performed on the remotely monitored host under the base or relay manager	{"sid":"_JP1IM_*integrated-manager-host-name*/_JP1IMBASEMGR_*base-or-relay-manger-host-name*/_JP1IMRM_*remotely-monitored-host-name*/_HOST_*remotely-monitored-host-name*/_JP1BASETRAP_","value":{...}},...

(2) Information retrieved from JP1/AJS

The following table lists the types and formats of the information retrieved from JP1/AJS.

Table 7–7: Types and formats of the information retrieved from JP1/AJS

Type of information	Format
The name of the host where JP1/AJS3 - Manager is installed	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*", "value":{...}},
JP1/AJS3 - Manager running on the host	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*/_JP1AJSMGR_, "value":{...}},

Type of information	Format
Scheduler service name (root job group)	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*/_JP1SCHE_*scheduler-service-name*", "value":{...}}, ...
The name of the running scheduler service	"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*/_JP1SCHE_*scheduler-service-name*/_JP1AJSSCHE_"
The name of the job group	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*/_JP1SCHE_*scheduler-service-name*/_JP1JOBG_*job-group-name*"}, "value":{...}}, ...
The name of the root jobnet	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_HOST_*AJS-manager-host-name*/_JP1SCHE_*scheduler-service-name*/_JP1JOBG_*job-group-name*/_JP1ROOTJOBNET_*root-jobnet-name*"}, "value":{...}}, ...
The name of the host where JP1/AJS3 - Agent under JP1/AJS3 - Manager is installed	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_JP1AJS-A_*AJS-agent-host-name*/_HOST_*AJS-agent-host-name*", "value":{...}}, ...
JP1/AJS3 - Agent under JP1/AJS3 - Manager running on the host	{"sid":"_JP1AJS-M_*AJS-manager-host-name*/_JP1AJS-A_*AJS-agent-host-name*/_HOST_*AJS-agent-host-name*/_JP1AJSAGT_", "value":{...}}, ...

(3) Information retrieved from JP1/PFM

The following table lists the types and formats of the information retrieved from JP1/PFM.

Table 7–8: Types and formats of the information retrieved from JP1/PFM

Type of information	Format
The name of the host where JP1/PFM - Manager is installed	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_HOST_*PFM-manager-host-name*","value":{...}},
JP1/PFM - Manager running on the host	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_HOST_*PFM-manager-host-name*/_JP1PFMMGR_","value":{...}},
The name of the host where JP1/PFM - Agent or JP1/PFM - RM is installed under JP1/PFM - Manager, and the name of the host monitored by JP1/PFM - RM	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_JP1PFM-AHOST_*PFM-agent-host-name*/_HOST_*PFM-agent-host-name*","value":{...}},...
JP1/PFM - Base that is installed on the host where JP1/PFM - Agent or JP1/PFM - RM is installed under JP1/PFM - Manager	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_JP1PFM-AHOST_*PFM-agent-host-name*/_HOST_*PFM-agent-host-name*/_JP1PFMBASE_","value":{...}},...
The service ID of JP1/PFM - Agent or JP1/PFM - RM under JP1/PFM - Manager	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_JP1PFM-AHOST_*PFM-agent-host-name*/_HOST_*PFM-agent-host-name*/_JP1PFM-A_*service-ID*","value":{...}},...
The service of JP1/PFM - Agent or JP1/PFM - RM under JP1/PFM - Manager	{"sid":"_JP1PFM-M_*PFM-manager-host-name*/_JP1PFM-AHOST_*PFM-agent-host-name*/_HOST_*PFM-agent-host-name*/_JP1PFM-A_*service-ID*/_JP1AGENTSERVICE_","value":{...}},...

(4) Information retrieved from JP1/NNMi

The following table lists the types and formats of information retrieved from JP1/NNMi.

Table 7–9: Types and formats of information retrieved from JP1/NNMi

Type of information	Format
Name of the host on which JP1/NNMi is installed	{"sid":"_JP1NNMI-M_*NNMi-manager-host-name*/_HOST_*NNMi-manager-host-name*","value":{...}},...
JP1/NNMi within the host	{"sid":"_JP1NNMI-M_*NNMi-manager-host-name*/_HOST_*NNMi-manager-host-name*/_JP1NNMiMGR_","value":{...}},...
Name of the node (other than network device) managed by JP1/NNMi	{"sid":"_JP1NNMI-M_*NNMi-manager-host-name*/_JP1NNMI-A_*NNMi-manager-host-name*/_HOST_*name-of-node-managed-by-NNMi*","value":{...}},...
Node (other than network device) managed by JP1/NNMi	{"sid":"_JP1NNMI-M_*NNMi-manager-host-name*/_JP1NNMI-A_*name-of-node-managed-by-NNMi*/_HOST_*name-of-node-managed-by-NNMi*/_NNMINODE_/","value":{...}},...
Name of the node (network device) managed by JP1/NNMi	{"sid":"_JP1NNMI-M_*NNMi-manager-host-name*/_JP1NNMI-A_*name-of-node-managed-by-NNMi*/_NETWORKDEVICE_*name-of-node-managed-by-NNMi*","value":{...}},...
Node (network device) managed by JP1/NNMi	{"sid":"_JP1NNMI-M_*name-of-node-managed-by-NNMi*/_JP1NNMI-A_*name-of-node-managed-by-NNMi*/_NETWORKDEVICE_*name-of-node-managed-by-NNMi*/_NNMINODE_/","value":{...}},...

(5) Information retrieved from JP1/OA

The following table lists the types and formats of information retrieved from JP1/OA.

Table 7–10: Types and formats of information retrieved from JP1/OA

Type of information	Format
Name of the host on which JP1/OA is installed	{"sid":"_JP1OA_*JP1/OA-host-name*/_HOST_*JP1/OA-host-name*","value":{...}},...
JP1/OA within the host	{"sid":"_JP1OA_*JP1/OA-host-name*/_HOST_*JP1/OA-host-name*/_JP1OAMGR_","value":{...}},...
Object monitored by JP1/OA (consumer)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*name-of-monitored-consumer*/_CONSUMER_*name-of-monitored-consumer*","value":{...}},...
Object monitored by JP1/OA (container cluster)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*name-of-cluster-in-monitored-container-environment*/_CONTAINERCLUSTER_*name-of-cluster-in-monitored-container-environment*","value":{...}},...
Object monitored by JP1/OA (container node)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*name-of-cluster-in-monitored-container-environment*/_CONTAINERCLUSTER_*name-of-cluster-in-monitored-container-environment*/_CONTAINERNODE_*name-of-node-in-monitored-container-environment*","value":{...}},...
Object monitored by JP1/OA (cluster)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*name-of-cluster-in-monitored-container-environment*/_SERVERCLUSTER_*monitored-cluster-name*","value":{...}},...
Object monitored by JP1/OA (hypervisor in cluster environment)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*name-of-cluster-in-monitored-container-environment*/_SERVERCLUSTER_*monitored-cluster-name*/_HYPERVISOR_*monitored-hypervisor-name*","value":{...}},...
Object monitored by JP1/OA (hypervisor)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-hypervisor-name*/_HYPERVISOR_*monitored-hypervisor-name*","value":{...}},...
Object monitored by JP1/OA (virtual machine)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-virtual-machine-name*/_VM_*monitored-virtual-machine-name*","value":{...}},...

Type of information	Format
Object monitored by JP1/OA (host)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-host-name*/_HOST_*monitored-host-name*","value":{...}},...
Object monitored by JP1/OA (IP switch)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-IP-switch-name*/_NETWORKDEVICES_*monitored-IP-switch-name*","value":{...}},...
Object monitored by JP1/OA (FC switch)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-FC-switch-name*/_NETWORKDEVICES_*monitored-FC-switch-name*","value":{...}},...
Object monitored by JP1/OA (storage system)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-storage-name*/_STORAGE_*monitored-storage-system-name*","value":{...}},...
Object monitored by JP1/OA (volume)	{"sid":"_JP1OA_*JP1/OA-host-name*/_JP1OA-A_*monitored-storage-name*/_STORAGE_*monitored-storage-name*/_STORAGEVOLUME_*monitored-volume-name*","value":{...}},...

(6) Information retrieved from JP1/SSO

The following table lists the types and formats of the information retrieved from JP1/SSO.

Table 7–11: Types and formats of the information retrieved from JP1/SSO

Type of information	Format
The name of the host where JP1/SSO is installed	{"sid":"_JP1SSO-M_*JP1/SSO-manager-host-name*/_HOST_*JP1/SSO-manager-host-name*","value":{...}},...
JP1/SSO on the host	{"sid":"_JP1SSO-M_*JP1/SSO-manager-host-name*/_HOST_*JP1/SSO-manager-host-name*/_JP1SSOMGR_","value":{...}},...
Host monitored by JP1/SSO (excluding network devices)	{"sid":"__JP1SSO-M_*JP1/SSO-manager-host-name*/_JP1SSO-A_*agent-host-name*/_HOST_*agent-host-name*","value":{...}},...
JP1/SSO agent in a host (excluding network devices)	{"sid":"__JP1SSO-M_*JP1/SSO-manager-host-name*/_JP1SSO-A_*agent-host-name*/_HOST_*agent-host-name*/_JP1SSOAGT_","value":{...}},...
Host monitored by JP1/SSO (network device)	{"sid":"__JP1SSO-M_*JP1/SSO-manager-host-name*/_JP1SSO-A_*agent-host-name*/_NETWORKDEVICE_*agent-host-name*","value":{...}},...
JP1/SSO agent in a host (network device)	{"sid":"__JP1SSO-M_*JP1/SSO-manager-host-name*/_JP1SSO-A_*agent-host-name*/_NETWORKDEVICE_*agent-host-name*/_JP1SSOAGT_","value":{...}},...

7.2 json objects

The following table lists json objects that can be accessed through the interface provided with the Intelligent Integrated Management Base.

Table 7–12: List of json objects

Category	Object name	Description	See
Event	Event information	An object to contain event information	*7.2.1(1)*
	Information for calling the monitor window of the linked product that issued an event	An object that represents the event information for calling the monitor window of the linked product	*7.2.1(2)*
	Event search condition	An object to contain event search conditions	*7.2.1(3)*
IM management node	IM management node tree information	An object to contain IM management node tree information	*7.2.2(1)*
	IM management node	An object to contain IM management node information	*7.2.2(2)*
	IM management node link master	An object to contain IM management node link master information	*7.2.2(3)*
Trend data management	Trend data	Trend data objects handled by the Trend Data Management Service.	*7.2.3(1)*
	Label Set List	A list object of label sets that can be obtained from Trend data Management Database through the Trend Data Management Service.	*7.2.3(2)*
Auto execution of Response Action	Auto Response Action Definition	An object representing the information about auto Response Action definition.	*7.2.4(1)*
Integrated agent Administration	Integrated agent Info	An object that represents information about the integration agent.	*7.2.5(1)*

7.2.1 Event

This section describes json objects for events.

(1) Event information object

Description

An object that contains event information

Format

```
{
    "sid":"JP1-event-SID",
    "value": [
        "event-attribute-name":"event-attribute-value",...
    ],
    "title": [
        "event-attribute-name":"display-name-of-the-event-attribute",...
    ],
    "type": [
        "event-attribute-name":"type-of-the-event-attribute",...
    ],
    "monitor": [
        information-for-calling-the-monitor-window-of-the-linked-product-t
hat-issued-an-event
    ]
}
```

Members

The following table describes the members of this object.

Table 7–13: Members of the event information object

No.	Member	Data type	Description
1	`sid`	string	Specifies the JP1 event SID that identifies the event uniquely. The format as follows: `_JP1IM_`*`manager-host-name`*`/_JP1IMSEQNO_`*`serial-number-in-the-integrated-monitoring-database`*`/_JP1IMEVBSEQNO_`*`serial-number-in-the-event-database`*
2	`value`	Object[]	Returns an array of pairs of event attributes and their values. If an attribute is not contained in the event, a string with the size of 0 bytes is returned as the attribute value. The format of the list of event attributes and the attribute values returned by the `value` parameter is equivalent to that of values in the database, except for the time type event attribute[#1] and IP-address event attribute[#2]. Event attributes of type time are returned in the ISO 8601 extended format (*YYYY*-*MM*-*DD*T*hh*:*mm*:*ssTZD*). When the event search API is run, this member returns event attributes that are specified with the `attrs` parameter. When the event detailed information acquisition API is run, this member returns event attributes according to the settings in the definition file for extended event attributes.
3	`title`	Object[]	Returns the list of event attributes and their display names. This member is returned when the event detailed information acquisition API is run. For details, see *5.6.2 Event detailed information acquisition*.
4	`type`[#3]	Object[]	Returns the list of event attribute names and attribute types. This member is returned when the event detailed information acquisition API is run. For details, see *5.6.2 Event detailed information acquisition*.
5	`monitor`	Object[]	Returns the information for calling the monitor window of the linked product that issued an event, if the event search API or event detailed information acquisition API is executed. For details, see *7.2.1(2) Object of the information for calling the monitor window of the linked product that issued an event*.

#1

Time type event attributes are the registered timeframe (`B.TIME`), arrived timeframe (`B.ARRIVEDTIME`), start timeframe (`E.START_TIME`), and end timeframe (`E.END_TIME`). Those attributes are output in the ISO 8601 extended format (*YYYY*-*MM*-*DD*T*hh*:*mm*:*ssTZD*). However, if start timeframe (`E.START_TIME`) and end timeframe (`E.END_TIME`) are non-numeric, or less than 0, they are output in string format.

#2

The event attribute of IP address type refers to the source IP address (`B.SOURCEIPADDR`) and the destination IP address (`B.DESTIPADDR`).

#3

The following table describes the attribute names and values returned by the `type` member:

No.	type	Description	Event attribute and relevant returned type
1	None	String The GUI is displayed in single-line text format.	Attributes that are not `text`, `html`, or `date`

No.	type	Description	Event attribute and relevant returned type
		Control characters (such as a line feed code) are replaced with space characters.	
2	text	String The GUI is displayed in multi-line text format (with the <pre> tag).	- Message (B.MESSAGE) - Post-change message (E.@JP1IM_DISPLAY_MESSAGE) - Memo (E.@JP1IM_MEMO) - Guide message in text format (E.@JP1IM_GUIDE)
3	html	HTML document The GUI is displayed in HTML format (with the <iframe> tag).	- Guide message in HTML format (E.@JP1IM_GUIDE)
4	date	String in ISO8601 format (2004-04-01T12:00+09:00) converted from date data. The GUI is displayed after the date is converted into the value in the timezone of the client (through new Date (value)).	Attribute of which either of the following is defined by the attr statement of the definition file for extended event attributes: - type="elapsed_time/date_format:CLIENT" - "elapsed_time_in_milli/date_format:CLIENT" In a JP1/IM event, it corresponds to the following attributes: - Registered timeframe (B.TIME) - Arrived timeframe (B.ARRIVEDTIME) - Start timeframe (E.START_TIME) - End timeframe (E.END_TIME) For details on the definition file for extended event attributes, see *Definition file for extended event attributes* in *Chapter 2. Definition Files*.

Important

In the REST API, the event attribute of a guide message is returned as an IM attribute (E.@JP1IM_GUIDE). The display name is shown as "ガイド" in Japanese and as Guide in English.

Event attributes of the consolidation start event

If the consolidateEvent request parameter of the event search API is set to true, the event attributes shown in the table below are set for the consolidation start event. They are not set for any event other than the consolidation start event. In addition, the event attributes of the consolidation start event are not output by the jcoevtreport command.

Table 7–14: Event attributes of the consolidation start event

No.	Attribute	Description
1	E.@JP1IM_CONSOLIDATION	Indicates whether the event is the consolidation start event. - 1: consolidation start event
2	E.@JP1IM_CONSOLIDATION_STATUS	Indicates the status of the consolidation start event. - 10: Normal/Resolved - 20: Warning/Notice/Information/Debug - 30: Error - 40: Emergency/Alert/Critical
3	E.@JP1IM_CONSOLIDATION_SEVERE_MIXED	Indicates whether the consolidation event contains a mix of severe and non-severe events. - 0: Not mixed - 1: Mixed
4	E.@JP1IM_CONSOLIDATION_DEALT_MIXED	Indicates whether event statuses of the consolidation event are mixed.

No.	Attribute	Description
		- 0: Not mixed - 1: Mixed
5	E.@JP1IM_CONSOLIDATION_ACTCONTROL_MIXED	Indicates whether statuses of automatic actions of the consolidation event are mixed. - 0: Not mixed - 1: Mixed

(2) Object of the information for calling the monitor window of the linked product that issued an event

Description

Is an object that represents the information for calling the monitor window of the linked product.

Format

```
{
   "url":"URL-of-the-window-of-the-linked-product"
}
```

Members

The following table describes the members of this object.

Table 7–15: Member of the object of the information for calling the monitor window of the linked product that issued an event

No.	Member	Data type	Description
1	`url`	string	URL of the window of the linked product

(3) Event search condition object

Description

This object contains event search conditions. An event is determined to match an event search condition object if the event does not match any of the exclusion condition groups and matches at least one of the pass condition groups.

Format

```
{
   "include":[pass-condition-group,...],
   "exclude":[exclusion-condition-group,...]
}
```

Format of a pass or exclusion condition group

Specify an array of a pass or exclusion condition group. Specified event conditions are joined with the AND operator.

```
[
{ "key":"event-attribute-name","ope":"comparison-condition","val":"operand
" },...
]
```

Members

The following table describes the members of this object.

Table 7–16: Members of the event search condition object

No.	Member	Data type	Description
1	include	Object[]	Specify 0 to 5 pass condition groups for event search. A pass condition group can contain 0 to 50 event conditions. For event conditions for extended attributes (specific information), a pass condition group can contain up to 5 conditions.
2	exclude	Object[]	Specify 0 to 5 exclusion condition groups for event search. An exclusion condition group can contain 0 to 50 event conditions. For event conditions for extended attributes (specific information), an exclusion condition group can contain up to 5 conditions.
3	key	string	Specify the name of an event attribute that you want to compare. To specify a basic attribute, prefix the name with `B.`. To specify an extended attribute (common information or specific information), prefix the name with `E.`. This member is case-sensitive. For the event attributes that are specifiable, see the *Attribute* column in *Table 7-17 Combination of acceptble attribute names and comparison keywords*.
4	ope	string	Specify a comparison operator for the event attribute specified with key. As a comparison operator, you can specify one of the following values: `BEGIN` (begins with), `IN` (matches), `NOTIN` (does not match), `SUBSTR` (includes), `NOTSUBSTR` (does not include), `REGEX` (regular expression), and `TRANGE` (date and time). This member is case-sensitive. The comparison conditions that can be specified for each event attribute are the same as those in the *Acceptable comparison keyword* column in *Table 7-17 Combination of specifiable attribute names and comparison keywords*. For details on the comparison conditions for the time type event attributes#, see *Table 7-18 Comparison conditions for time type event attributes* and *Table 7-19 List of time type event attributes*.
5	val	The value depends on key.	Specify a value (operand) to be compared against the value of the event attribute specified with `key`. This member is case-sensitive. When multiple operands are allowed, specify them as an array of operands. When multiple operands are specified, the OR condition is used. However, when a regular expression is specified as a comparison keyword, the specification of multiple operands is not allowed. Even if the operand accepts multiple specifications, an empty array or an array with `null` specified for an element cannot be specified. When a half-width space character, a tab character, a line feed/carriage return character (CR or LF), or a percent sign (%) is used to specify an operand, it must be written as follows: • Half-width space character (0x20): `%20` • Tab character (0x09): `%09` • Line feed code (LF) (0x0a): `%0a` • Carriage return code (CR) (0x0d): `%0d` • Percent sign (%) (0x25): `%25` You can specify a maximum of 4,096 bytes of operands per event condition and per event condition block (total length in bytes of all operands that are specified in the event condition block). The comparison values (operands) that can be specified for each event attribute are the same as those in the *Operand* column in *Table 7-17 Combination of acceptble attribute names and comparison keywords*. Specify an array of operands if multiple operands are allowed.

#

Time type event attributes are the registered timeframe (`B.TIME`), arrived timeframe (`B.ARRIVEDTIME`), start timeframe (`E.START_TIME`), and end timeframe (`E.END_TIME`).

Table 7–17: Combination of acceptable attribute names and comparison keywords

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
1	Basic attribute	Event ID (B.ID)	Numeric	• Match • Does not match	Multiple values are allowed. The maximum number of values you can specify is 100. Values must be specified in hexadecimal notation. The letters are case insensitive. However, letters in a regular expression are case sensitive. The acceptable range is from 0 to 7FFFFFFF.
2		Registered reason (B.REASON)	Numeric	• Match • Does not match	Multiple values are allowed. The maximum number of values you can specify is 100.
3		Source process ID (B.PROCESSID)	Numeric	• Match • Does not match	Multiple values are allowed. The maximum number of values you can specify is 100. The acceptable range is from -2147483648 to 2147483647.
4		Source user ID (B.USERID)	Numeric	• Match • Does not match	Multiple values are allowed. The maximum number of values you can specify is 100. The acceptable range is from -2147483648 to 2147483647.
5		Source group ID (B.GROUPID)	Numeric		
6		Source user name (B.USERNAME)	String	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
7		Source group name (B.GROUPNAME)	String		
8		Source event server name (B.SOURCESERVER)	String		
9		Destination event server name (B.DESTSERVER)	String		
10		Message (B.MESSAGE)	String	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
11		Registered timeframe (B.TIME)	Time	• Time	Specify the start date and time and end date and time of a period. A match occurs if the start data and time <= time <= end date and time is true.
12		Arrived timeframe (B.ARRIVEDTIME)	Time	• Time	
13	Extended attribute	Event level (E.SEVERITY)	String	• Match	Multiple values are allowed. Note that one level can be specified only once.

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
	(common information)				Acceptable values: Emergency, Alert, Critical, Error, Warning, Notice, Information, and Debug.
14		User name (E.USER_NAME)	String	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
15		Product name (E.PRODUCT_NAME)	String		
16		Object type (E.OBJECT_TYPE)	String		
17		Object name (E.OBJECT_NAME)	String		
18		Root object type (E.ROOT_OBJECT_TYPE)	String		
19		Root object name (E.ROOT_OBJECT_NAME)	String		
20		Object ID (E.OBJECT_ID)	String		
21		Occurrence (E.OCCURRENCE)	String		
22		Start timeframe (E.START_TIME)	String	• Time	Specify the start date and time and end date and time of a period. A match occurs if the start data and time <= time <= end date and time is true.
23		End time (E.END_TIME)	String	• Time	
24		Result code (E.RESULT_CODE)	String	• First characters • Match • Does not match • Is contained • Is not contained • Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
25		Event source host name (E.JP1_SOURCEHOST)	String		
26	Extended attribute (specific information)	E.*attribute	String	• First characters • Match • Does not match • Is contained • Is not contained	An attribute name must begin with an uppercase alphabetical letter and be composed of uppercase alphabetical letters, numbers, and underscores (_). The maximum length is 32 bytes. Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
				- Regular expression	
27	IM attribute	Action type (E.@JP1IM_ACTTYPE)	Numeric	- Match - Does not match	- The following numeric values can be specified: 0: Not subject to an action 1: Command - Multiple values are allowed.
28		Action suppression (E.@JP1IM_ACTCONTROL)	Numeric		- The following numeric values can be specified: 0: Not subject to an action 1: Execution 2: Suppression 3: Partial suppression - Multiple values are allowed.
29		Severe event (E.@JP1IM_SEVERE)	Numeric		- The following numeric values can be specified: 0: Not a severe event 1: Severe event - Multiple values are allowed.
30		Correlation event (E.@JP1IM_CORRELATE)	Numeric		- The following numeric values can be specified: 0: Not a correlation event 1: Correlation approval event 2: Correlation failure event - Multiple values are allowed.
31		Response-waiting event (E.@JP1IM_RESPONSE)	Numeric		- The following numeric values can be specified: 0: Not a response waiting event 1: Response waiting event - Multiple values are allowed.
32		Original severity level (E.@JP1IM_ORIGINAL_SEVERITY)	String	- First characters - Match - Does not match - Is contained - Is not contained - Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. However, if a regular expression is used, only one value is allowed.
33		New severity level (E.@JP1IM_CHANGE_SEVERITY)	Numeric	- Match - Does not match	- The following numeric values can be specified: 0: No new severity level exists 1: New severity level exists - Multiple values are allowed.

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
34		Event status (E.@JP1IM_DEALT)	Numeric		- The following numeric values can be specified: 0: Unprocessed 1: Processed 2: Processing 3: Held - Multiple values are allowed.
35		Severe event released (E.@JP1IM_RELEASE)	Numeric		- The following numeric values can be specified: 0: No severe events are released 1: Severe events are released - Multiple values are allowed.
36		Severe event deleted (E.@JP1IM_DISMISSED)	Numeric		- The following numeric values can be specified: 0: No severe events are deleted 1: Severe events are deleted - Multiple values are allowed.
37		Memo (E.@JP1IM_MEMO)	String	- First characters - Match - Does not match - Is contained - Is not contained - Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
38		Changed display message (E.@JP1IM_DISPLAY_MESSAGE)	String	- First characters - Match - Does not match - Is contained - Is not contained - Regular expression	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.
39		New display message (E.@JP1IM_CHANGE_MESSAGE)	Numeric	- Match - Does not match	The acceptable range is from -2147483648 to 2147483647.
40		Display message change definition name (E.@JP1IM_CHANGE_MESSAGE_NAME)	String	- First characters - Match - Does not match - Is contained	Multiple values are allowed. The maximum number of values you can specify is 100. For Regular expression, however, only one regular expression is allowed.

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
				- `Is not contained` - `Regular expression`	

Legend:

None: Cannot be compared.

--: N/A

Table 7–18: Comparison conditions for time type event attributes

No.	Comparison keyword	Data type	Description
1	Time (`TRANGE`)	Specify the start date and time and end date and time.	A JP1 event attribute (time type) is determined to satisfy an event condition when the attribute value falls in a range specified with the operands (start date and time and end date and time). The operands must be specified in the ISO 8601 extended format. Time range to be specified Start date and time <= Attribute value <= End date and time Time format *YYYY*-*MM*-*DD*`T`*hh*`:`*mm*`:`*ssTZD* Example To specify a range from March 1 to March 31, 2018: `{"key":"B.TIME","ope":"TRANGE","val":["2018-03-01T00:00:00+09:00","2018-03-31T00:00:00+09:00"]}`

Table 7–19: List of time type event attributes

No.	Type	Attribute	Data type	Acceptable comparison keyword	Operand
1	Basic attribute	Registered timeframe (`B.TIME`)	Time	`Time`	The operand can be specified in the same way as shown in *Table 7-18 Comparison conditions for time type event attributes*.
2		Arrived timeframe (`B.ARRIVEDTIME`)	Time	`Time`	
3	Extended attribute	Start timeframe (`E.START_TIME`)	Time	`Time`	
4		End timeframe (`E.END_TIME`)	Time		

7.2.2 IM management node

This section describes json objects for IM management node information.

(1) IM management node tree object

Description

An object that contains the information of an IM management node tree

Format

```
{
  "meta":{
    "format":"file-type",
    "timestamp":"file-created-time"
    "componentName":"component-name",
    "hostName":"host-name",
    "version":"1"
  },
  "simtData":[
    {"sid":"IM-management-node-tree-SID"},...
  ]
}
```

Members

The following table describes the members of this object.

Table 7–20: Members of the IM management node tree object

No.	Member	Data type	Description
1	`meta`	array	An array that stores file information
2	`format`	string	The file format. This is always set to `conf.` This attribute cannot be omitted.
3	`timestamp`	string	Returns the date and time when the file was created, as a UTC date time value in the ISO 8601 format. This attribute cannot be omitted. The time is based on the time of the JP1/IM - Manager server.
4	`compornentName`	string	Specifies the name of the component from which IM management node information is retrieved.
5	`hostName`	string	Specifies the name of the host from which IM management node information is retrieved.
6	`version`	string	The version of the file. Always set this to `1`.
7	`simtData`	array	An array that stores the SIDs of IM management nodes. You can specify the SID of the IM management node for `target`, the label to be displayed for `label`, and the image file to be displayed as the node icon on the **Related node** tab for `iconName`, which together constitute the `value` of the tree SID. For details about the names of image files, see *2.6.1 (7) Icons for related nodes* in the *JP1/Integrated Management 3 - Manager GUI Reference*.
8	`sid`	string	Specifies the tree SID of the IM management node.

Output example

```
{
  "meta":{
    "format":"conf"
    "timestamp":"2018-11-11T00:00:00Z"
     "componentName":"/HITACHI/JP1/IMDD"
     "hostName":"host1"
  },
  "simtData":[
    {"sid":"_ROOT_AllSystems","value":{"target":[],"iconName":"ROOT.png","
label":"All Systems"}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1","value":{"target":[],"label"
:"system1",...}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1","value":{
"target":[],"label":"sub-system1",...}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HOST_host
1","value":{"target":[],"label":"host1",...}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HOST_host
1/_CATEGORY_job","value":{"target":[],"label":"Job",...}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HOST_host
1/_CATEGORY_job/_SUBCATEGORY_JP1%2FAJS3%20-%20Manager/_OBJECT_AJSROOT1/_OB
JECT_jobgroup","value":{"target":[],"label":"jobgroup",...}},
    {"sid":"_ROOT_AllSystems/_SYSTEM_System1/_SYSTEM_SubSystem1/_HOST_hos
t1/_CATEGORY_job/_SUBCATEGORY_JP1%2FAJS3%20-%20Manager/_OBJECT_AJSROOT1/_O
BJECT_jobgroup/_OBJECT_jobnet1","value":{"target":[],"label":"jobnet1",...
}}
  ]
}
```

(2) IM management node object

Description

An object that contains IM management node information

Format

```
{
  "meta":{
    "format":"file-type",
    "timestamp":"file-created-time"
    "componentName":"component-name",
    "hostName":"host-name",
    "version":"1"
  },
  "simtData":[
    {"sid":"IM-management-node-SID"},...
  ]
}
```

Members

The following table describes the members of this object.

Table 7–21: Members of the IM management node object

No.	Member	Data type	Description
1	`meta`	array	An array that stores file information
2	`format`	string	The file format. This is always set to `conf`. This attribute cannot be omitted.
3	`timestamp`	string	Returns the date and time when the file was created, as a UTC date time value in the ISO 8601 format. This attribute cannot be omitted. The time is based on the time of the JP1/IM - Manager server.

No.	Member	Data type	Description
4	`compornentName`	string	Specifies the name of the component from which IM management node information is retrieved. It accepts alphanumeric characters and a forward slash (`/`).
5	`hostName`	string	• For the IM management node object file Specifies the name of the host from which IM management node information is retrieved. • For the IM management node object master file Always set this to `master`.
6	`version`	string	The version of the file. Always set this to `1`.
7	`simtData`	array	An array that stores the SIDs of IM management nodes.
8	`sid`	string	Specifies the SID of the IM management node.

Output example

```
{
  "meta":{
    "format":"conf"
    "timestamp":"2018-11-11T00:00:00Z"
    "componentName":"/HITACHI/JP1/AJS3/CONFINFO"
    "hostName":"host1"
  },
"simtData":[
    {"sid":"_JP1AJS-M_host1/_HOST_host1","value":{...}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv","value":{.
..}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jo
bgroup","value":{...}},
    {"sid":"_JP1AJS-M_host1/_HOST_host1/_JP1SCHE_schedulerserv/_JP1JOBG_jo
bgroup/_JP1ROOTJOBNET_jobnet1","value":{...}},
    {"sid":"_JP1AJS-M_host1/_JP1AJS-A_AGT10/_HOST_host10","value":{...}},
    {"sid":"_JP1PFM-M_host2/_HOST_host2","value":{...}},
    {"sid":"_JP1PFM-M_host2/_JP1PFM-A_servid/_HOST_host20","value":{...}}
  ]
}
```

(3) IM management node link master object

Description

An object that contains the information of an IM management node link master.

Format

```
{
    "meta":{
      "format":"file-type",
      "timestamp":"file-created-time"
      "componentName":"component-name",
      "hostName":"host-name",
      "version":"1"
    },
    "links": [
        {
        "from": "preceding-node-SID",
        "to": "succeeding-node-SID",
        "type": "type-of-the-target"
        }, ...
    ]
}
```

Members

The following table describes the members of this object.

Table 7–22: Members of the IM management node link master object

No.	Member	Data type	Description
1	`meta`	array	An array that stores file information
2	`format`	string	The file format. This is always set to `conf`. This attribute cannot be omitted.
3	`timestamp`	string	Returns the date and time when the file was created, as a UTC date time value in the ISO 8601 format. This attribute cannot be omitted. The time is based on the time of the JP1/IM - Manager server.
4	`compornentName`	string	Always set this to `master`.
5	`hostName`	string	Always set this to `master`.
6	`version`	string	The version of the file. Always set this to `1`.
7	`links`	array	An array for the response object. The order of the array is irrelevant.
8	`from`	string	The preceding node. It specifies the SID of the preceding node. This attribute cannot be omitted. Example: When a root jobnet is specified: `_JP1AJS-M_`*JP1/AJS3-manager-host-name*`/_HOST_`*JP1/AJS3-manager-host-name*`/_JP1SCHE_`*scheduler-service-name*`/_JP1JOBG_`*job-group-name*`/_JP1ROOTJOBNET_`*node-name*
9	`to`	string	The succeeding node. It specifies the SID of the succeeding node. This attribute cannot be omitted. Example: When a root jobnet is specified: `_JP1AJS-M_JP1/`*AJS3-manager-host-name*`/_HOST_`*JP1/AJS3-manager-host-name*`/_JP1SCHE_`*scheduler-service-name*`/_JP1JOBG_`*job-group-name*`/_JP1ROOTJOBNET_`*node-name*
10	`type`	string	Specify the type of the link information that you want to retrieve, among the link information types applied to the system. `type` describes a grouping of relations that have the same meaning. On the **Related node** tab in the Integrated Operation Viewer window, you can filter relations to display only those belonging to a specific type. For relations within a JP1/IM product or between a JP1/IM product and another product, the following types are used. In addition to these types, the use of user-specified types is also allowed. • `rootJobnetExecutionOrder`: relation of the execution order of root jobnets • `managerAgent`: Relation between the manager and agent of a JP1 product • `rootJobnetAgent`: Relation between a root jobnet and an AJS agent • `sameNode`: Relation between nodes with the same name • `L2Connection`: Relation between layer-2 connection lines managed by JP1/NNMi • `Infrastructure`: Relation between infrastructure resources managed by JP1/OA

No.	Member	Data type	Description
			• `monitoringConfiguration`: Relation between a product and a monitoring target in a monitoring product configuration

Output example

```
{
 "meta":{
    "format":"conf"
    "timestamp":"2018-11-11T00:00:00Z"
        "componentName":"AJS"
        "hostName":"host1"
  },
    "links": [
        {
        "from": "preceding-node-SID",
        "to": "succeeding-node-SID",
        "type": "type-of-the-target"
        }, ...
    ],
}
```

7.2.3 Trend Data Management

(1) Trend Data Object

Description

A json representing the trend data held by Trend data Management Database.

When the jp1trendDataService.getTrendData method is executed from the product plug-in, the trend data object is returned as the return data object via the trend data management service (Promscale).

For details of jp1TrendDataService.getTrendData method, see *4.5.17 jp1TrendDataService.getTrendData*.

Format

```
{
  "status":"status",
  "data":{
     "resultType":"result-type",
     "result":[
       {"metric":{
         "Label-name":"label-value",
         ...
         },
        "values":[
          [time,"value"],
          ...
          ]
       }
     ]
  }
}
```

Members

Members are listed in the following table.

Table 7–23: Trend data object members

No.	Member	Data type	Description
1	status	string	A string that represents the retrieved result. If the acquisition is successful, "success" is set.
2	resultType	string	A string that represents the type of data retrieved. Fixed "matrix" is set.
3	result	array	An array that represents the trend data.
4	metric	array	An array that contains the labels attached to the trend data.
5	*label name*	*string*	*The name of the label given to the trend data.*
6	*label value*	string	The value of the label given to the trend data.
7	values	array	An array that represents the performance data for each time.
8	time	Numeric	The time of the performance data (the number of seconds elapsed since January 1, 1970 00:00:00 UTC).
9	values	Numeric	The value of the performance data.

Output example

```
{
  "status":"success",
  "data":{
     "resultType":"matrix",
     "result":[
       {"metric":{
         "__name__":"foo",
         "job":"hoge"
         },
        "values":[
          [1617436800,"100"],
          [1617436830,"100"],
          [1617436860,"100"],
          [1617436890,"100"]
          ]
       }
     ]
  }
}
```

(2) Label Set List Object

Description

A json object that lists the label sets for trend data held by Trend data Management Database.

When you Execute jp1trendDataService.getLabelList method from product plugin, the label set list object is returned as a data object for the return Value through the Trend Data Management Service (Promscale).

For Detail of jp1TrendDataService.getLabelList method, see *4.5.18 jp1TrendDataService.getLabelList*.

Format

```
{
  "status":"Status",
  "data":[
       {
         "Label name":"Label Value",
         ...
       },
       {
         "Label name":"Label Value",
         ...
       },
       ...
  ]
}
```

Within the above definition, the following part shows a single set of labels.

```
       {
         "Label name":"Label Value",
         ...
       },
```

Members

Members are listed in the following table.

Table 7–24: Trend data object members

No.	Member	Data type	Description
1	`status`	`string`	A character string representing the result of the acquisition. If the acquisition is successful, "success" is Setup.
2	*Label name*	`string`	The name of the label attached to the trend data.
3	*Label Value*	`string`	The value of the label attached to the trend data.

Output example

```
{
   "status" : "success",
   "data" : [
      {
         "__name__" : "up",
         "job" : "prometheus",
         "instance" : "localhost:9090"
      },
      {
         "__name__" : "up",
         "job" : "node",
         "instance" : "localhost:9091"
      }
   ]
}
```

7.2.4 Auto execution of response action

(1) Auto Response Action definition Object

Description

An json object representing information about automated Response action definition. The size of this object is limited to less than 10MB.

Format

```
{
  "meta":{
    "version":"Version information"
  },
  "actions":[
    {"actionGroup":"Action grouping",
     "actionId":"Action ID",
     "label":"Action name",
     "description":"Comment",
     "valid":"Enable /Disable",
     "conditions":[
       {"type":"type",
        "key":"Attribute name",
        "ope":"Operators",
        "val":["Attribute value",...]
       },
       ...
     ],
     "action":{
       "type":"Action type",
       "params":"Action Description"
     }
    },
  ...
  ]
}
```

When specifying a character string in the items in the above definition, if `"` or `\` is included as a normal character, it is preceded by `\`, and it is set to `\"`, `\\`.

Definitions

Members

Members are listed in the following table.

Table 7–25: Members of Auto Response Action Definition Objects

No.	Member		Data type	Needing to specify	Description
1	meta		object	Required	Objects that Setup Common data for the entire auto response Action
2		version	string	Required	Specify Version. Specify 1 as the fixed Value.
3	actions		object[]	Optional	Array of auto Response Action Setup that Setup the conditions that trigger Response Action to Execute and Execute content of Response Action

No.	Member			Data type	Needing to specify	Description
						The number of items that can be specified is 0 to 1000 (the default Value).
4		actionGroup		int	Required	specifies the number of the Response Action grouping as an integer from 0 to 9. The size of the number in Response Action group is independent of the precedence of Execute conditional determination and Response Action's Execute condition. You can specify one execution of Response Action per group, allowing you to execute up to 10 Response Action at the same time for a single system status change.
5		actionId		int	Required	Specifies Action ID to be uniquely allocated for each automated ResponseAction Setup. Value can be an integer from 0 to 2,147,483,647.
6		label		string	Required	Specifies Action name to identify the auto Response Action Setup as a character string from 1 to 50 bytes. You can specify any character other than the control character (0x00 to 0x1F,0x7F to 0x9F).
7		description		string	Optional	Specify Comment (explanation of Response Action to Execute) for the auto Response Action Setup as a character string from 1 to 1040 bytes. You can specify any character other than the control character (0x00 to 0x1F,0x7F to 0x9F). This field has no effect on auto execution of response Action.
8		valid		boolean	Optional	Specifies whether to Enable the applicable auto Response Action Setup. • True: Enable • False: Disabled By default, "true" is used.
9		conditions		object[]	Required	Specifies the criteria that triggers execution of Response Action. The number of conditions that can be specified is 1 to 256. If more than one execution condition is specified, it is determined that execution condition is Match when all event conditions are met (AND condition).
10			type	string	Required	Specifies type of execution criteria. Specify "event" as the fixed Value.
11			key	string	Required	Specifies Attribute name of execution criteria. The following Attribute name can be specified: • B.ID (Event ID) • B.REASON (Registered reason) • B.PROCESSID (Source user ID) • B.USERID (Source user ID) • B.GROUPID (Source group ID) • B.TIME (Registered time) • B.ARRIVEDTIME (Arrived time) • B.USERNAME (Source user name) • B.GROUPNAME (Source group name) • B.SOURCEIPADDR (Source IP address) • B.SOURCESERVER (Source event server name) • B.MESSAGE (Message) • E. START_TIME (Start time)

No.	Member			Data type	Needing to specify	Description
						• E.END_TIME (End time) • E.PRODUCT_NAME (Product name) • E.OBJECT_TYPE (Object type) • E.OBJECT_NAME (Object name) • E.ROOT_OBJECT_TYPE (Root object type) • E.ROOT_OBJECT_NAME (Root object name) • E.OBJECT_ID (Object ID) • E.OCCURRENCE (Occurrence) • E.USER_NAME (User name) • E. RESULT_CODE (Result code) • E.SEVERITY (Event level) • E.* (Unique extended attributes) • E.@JP1IM_DISPLAY_MESSAGE (Display Message)
`12`			`ope`	`string`	Required	Specifies the criteria for comparing Attribute name specified in key. The comparison condition can be one of the following: • BEGIN (starts with) • IN (Match to) • NOTIN (not Match with) • SUBSTR (including) • NOTSUBSTR (not including) • REGEX (regular expressions) For details about the comparison conditions that can be specified for each Attribute name, see the table ■*Combination of Setup Value that can be specified in execution criteria* below.
`13`			`val`	`string[]`	Required	Specifies the compare Value (string) of Attribute name specified in key. It is case sensitive. If you do not specify regular expressions for the compare Value, you can specify more than one (up to 100). If more than one condition is specified, it is determined as execution condition has matched when Match has occurred in one of the conditions (OR condition). The comparison Value can be a string that meets the following criteria: • Up to 4096 bytes per compare Value, up to a total of 4096 bytes (total bytes of compare Value described in Execute condition) per execution condition • Compare Value of Attribute name specified in key For details about the comparison conditions that can be specified for each Attribute name, see the table ■*Combination of Setup Value that can be specified in execution criteria* below.
`14`		`action`		`object`	Required	Objects that Setup the content of execution when it is Match in execution criteria
`15`			`type`	`string`	Required	Specifies type of Action to Execute. • Cmd : Specifies that OS command is to Execute. • Restapi: Specifies that REST API is to Execute.
`16`			`params`	object	Required	Specifies the content of Action to Execute. This field can be an Value that contains event-takeover credentials. • When type of Action is "cmd"

No.	Member	Data type	Needing to specify	Description
				For the members that can be specified, see the table ■*Members that can be specified when type is cmd* below. • When type of Action is "restapi" For the members that can be specified, see the table ■*Members that can be specified when type is restapi* below.

■Combination of Setup Value that can be specified in execution criteria

Key(Attribute name)	Type"	Ope (Compare)	Val (Compare Value)
B.ID (Event ID)	Numeric	• IN (Match to) • NOTIN (not Match with)	You specify Event ID. • Case is not distinguished. • The range is 0 to 7FFFFFFFF. • When Event ID basic part or Event ID extension part is a Value of less than 8 digits, the leading part is padded with 0s and the character string is going to be 8 digits.
B.REASON (Registered reason)	Numeric		Specifies registered reason. • The range is -2,147,483,648 to 2,147,483,648.
B.PROCESSID (Source process ID)	Numeric		Specifies the process ID of the issuing application. • The range is -2,147,483,648 to 2,147,483,648.
B.USERID (Source user ID)	Numeric		Specifies the numerical ID of the issuing process. • The range is- 2,147,483,648 to 2,147,483,648.
B.GROUPID (Source group ID)	Numeric		Specifies the group ID (number) of the issuing process. • The range is -2,147,483,648 to 2,147,483,648.
B.TIME (Registered time)	Time	REGEX (regular expressions)	Specifies the time that JP1 event was registered to event database of the issuing host. • You specify in regular expressions in the form of *YYYYMMDDhhmmss*.
B.ARRIVEDTIME (Arrived time)	Time		Specifies the time JP1 event arrived at the issuing host's event database. • You specify in regular expressions in the form of *YYYYMMDDhhmmss*.
B.USERNAME (Source user name)	String	• BEGIN (starts with) • IN (Match to) • NOTIN (not Match with) • REGEX (regular expressions)	Specifies User name of the issuing process.
B.GROUPNAME (Source group ID)	String		Specifies the group name of the issuing process.
B.SOURCEIPADDR (Source IP address)	String		Specifies IP address corresponding to the issuing event Server. For details about IP address specification format, see ■*Value that can be specified in execution crieteria of Action* below.
B.SOURCESERVER (Source event server name)	String		Specifies Host name (event Server) of the host where JP1 event occurred.
B.MESSAGE (Message)	String		Specifies Message of the event base attribute.
E.START_TIME (Start time)	String	REGEX (regular expressions)	Specifies the time of start or restart of execution. • Specify in the regular expression specification of total seconds.

Key(Attribute name)	Type"	Ope (Compare)	Val (Compare Value)
E.END_TIME (End time)	String		Specifies the time when execution ends. • Specify in the regular expression specification of total seconds.
E.PRODUCT_NAME (Product name)	String	• BEGIN (starts with) • IN (Match to) • NOTIN (not Match with) • SUBSTR (including) • NOTSUBSTR (not including) • REGEX (regular expressions)	Specifies the name of the programs that issued JP1 event.
E.OBJECT_TYPE (Object type)	String		Specifies the type of JP1 event object.
E.OBJECT_NAME (Object name)	String		Specifies object name of JP1 event.
E.ROOT_OBJECT_TYPE (Root object type)	String		Specifies Root object type of JP1 event.
E.ROOT_OBJECT_NAME (Root object name)	String		Specifies Root object name of JP1 event.
E.OBJECT_ID (Object ID)	String		Specifies Object ID of JP1 event.
E.OCCURRENCE (Occurrence)	String		Specifies Occurrence of JP1 event.
E.USER_NAME (User name)	String		Specifies username that issued JP1 event.
E.RESULT_CODE (Result code)	String		Specifies an exit code.
E.SEVERITY (Event level)	String	• IN (Match to) • REGEX (regular expressions)	Specifies Event level of JP1 event. • When you set IN (match to) in Ope, specify in one of "Emergency", "Alert", "Critical", "Error", "Warning", "Notice", "Information", or "Debug".
E.* (Unique extended attributes)	String	• BEGIN (starts with) • IN (Match to) • NOTIN (not Match with) • SUBSTR (including) • NOTSUBSTR (not including) • REGEX (regular expressions)	Specify Value of Attribute name specified in the E.* format in key.
E.@JP1IM_DISPLAY_MESSAGE (Display message)	String		Specifies Message of IM attribute in JP1 event.

■Value that can be specified in execution criteria of Action

For Source IP address event conditions, in addition to IPv4 address conditions, you can specify IPv6 address conditions in IPv6 address notation (alphabetic characters in IPv6 notation must be specified in lowercase).

The following table lists IP address conditions that can be specified for Source IP address event conditions:

Source IP address	**Example of specification**	**Can be specified?**
IPv4 addressing	`11.22.33.44`	Yes
IPv6 addressing	`0011:2233:4455:6677:8899:aabb:cccdd:eeff`	Yes
	`0011:2233:4455:6677:8899:AABB:CCDD:EEFF`	No

Source IP address		Example of specification	Can be specifie d?
		`2012:7:8::a:b`	No
Special IPv6 address	IPv4 projection addressing	`::ffff:11.22.33.44`	No
	IPv6 projection addressing	`::11.22.33.44`	No

■Members that can be specified when type is cmd

Member name	Data Type	Can be specified?	Description
`host`	string	Required	Specify execution destination Host name of the command. The range is 1 to 255.
`cmd`	string	Required	Specify Command and arguments between 1 and 4096 bytes. If the command name contains spaces, enclose it in double quotation marks (").
`envFile`	string	Optional	Specifies the absolute path of Environment variable file of execution destination, from 1 to 255. For details about Environment variable file, see *Environment variable file (any file name)* in *Chapter 2. Definition Files*.

■Members that can be specified when type is restapi

Member name	Data Type	Can be specified?	Description
`method`	string	Required	Specifies the method of REST API.
`url`	string	Required	Specifies URL of REST API. When the URL including host name is specified, register the host name to the integrated manager's `hosts` file and DNS so as to enable name resolution on the integrated manager host. Configuration in the `jp1hosts` file and the `jp1hosts2` file are not referred.

`headers`	object	Required	Specify the request header for REST API in the following format:
			`{`
			`"`*Element-name-1*`":  "`*Value of the element 1*`",`
			`"`*Element name 2*`";  "`*Value of the element 2*`"`
			`}`

`body`	string	Optional	Specifies the request body of REST API in any string-format.

Output example

```
{
  "meta":{
    "version":"1"
  },
  "actions":[
    {"actionGroup":0,
     "actionId":"0",
     "label":"Event error for collecting data",
     "description":"To execute collecting data when an error is detected b
y a particular Event ID",
     "valid":true,
     "conditions":[
       {"type":"event",
        "key":"B.ID",
        "ope":"IN",
        "val":["00004860","00004861"]
       },
       {"type":"event",
        "key":"E.SEVERITY",
        "ope":"IN",
        "val":["Error","Emergency"]
       }
     ],
     "action":{
       "type":"cmd",
       "params":{
         "host":"${event:EVHOST:}",
         "cmd":"\"C:\\Program Files (x86)\\Hitachi\\JP1IMM\\tools\\jim_log
\" -f C:\\temp -q",
         "envFile":"C:\\tmp\\envFile.txt"
       }
     }
    }
  ]
}
```

7.2.5 Integrated agent administration

(1) Integrated agent Info object

Description

A json object representing integrated agent info.

Format

```
{
  "agentid": agent ID,
  "agenthost": integrated agent host name,
  "os": OS name,
  "installpath": Installation path,
  "imversion": version of integrated agent,
  "managerhost" Manager Host name,
  "registeredtime" registration date and time,
  "addons": [
    {
      "addonName": Function name,
      "enabled ": Status
    }, ...
  ]
}
```

Members

Members are listed in the following table.

Table 7–26: Members of integrated agent info object

No.	Member	Data type	Description
1	agentid	string	Specifies ID of integrated agent.

No.	Member		Data type	Description
2	agenthost		string	Specifies Host name of integrated agent.
3	os		string	Specifies OS of the host for integrated agent. (Ex: windows, linux)
4	installpath		string	Specifies Installation path of JP1/IM - Agent installed on integrated agent host.
5	imversion		string	Specifies Version (VVRRSS) of JP1/IM - Agent as a six-digit number.
6	managerhost		string	Specifies Host name of integrated agent manager.
7	registeredtime		string	Specifies UTC time in ISO 8601 format as the registration date and time of integrated agent data. The registration date and time will be updated when JP1/IM - Agent is started after the following operations are performed: • Installation of JP1/IM - Agent • Version upgrade install of JP1/IM - Agent • Delete JP1/IM - Agent on the JP1/IM agent list screen of the Integrated Operation Viewer
8	addons		object[]	Specifies an array of add-on information objects.
9		addonName	string	Specify the add-on name.
10		enabled	boolean	Specify whether to Enable the add-on function. • True: Enabled • False: Disabled

Output example

```
{
  "agentid": "RENEMzNENDg5RkQyNEM2OT",
  "agenthost": "agenthostA",
  "os": "windows",
  "installpath": "C\\Program Files\\Hitachi\\jp1ima",
  "imversion": "130000",
  "managerhost": "managerhostA",
  "registeredtime": "2020-03-01T00:00:00Z",
  "addons": [
    {
      "addonName": "Windows metric collector(Windows exporter)",
      "enables": true
    }, ...
  ]
}
```

7.3 Configuring the adapter command

This chapter describes the configuration of the adapter command.

Note that JP1/Base is needed for the execution environment of the adapter command.

7.3.1 Setting up the adapter command

(1) Setup

1. Execute the setup command provided by each linked product.
2. The adapter command settings file is generated in the following location:

   In Windows:

   JP1/Base-installation-folder[#]`\plugin\conf`

   In UNIX:

   `/opt/jp1base/plugin/conf`

   #

   The folders below are the default installation locations for each product. Note that *system-drive*`:\ProgramData` represents the location determined by the OS environment variable during installation, and thus it may vary depending on your environment.

   In an x86 environment: *system-drive*`:\Program Files\Hitachi\JP1Base`

   In an x64 environment: *system-drive*`:\Program Files (x86)\Hitachi\JP1Base`

Important

- In Windows, the installation directory of JP1/Base is retrieved from the following registry entry:
  `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\JP1BASE\PATHNAME\PATH00`
- If there is a file with the same name at the location where the file is to be stored, the file is overwritten.
- Do not stop the JP1/Base service.

(2) Unsetup

1. Execute the unsetup command provided by each linked product.
2. Remove the adapter command settings file manually.

Important

- Do not stop the JP1/Base service.
- When you uninstall a linked product, the adapter command settings file is also uninstalled.

7.3.2 Adapter command settings file

This section describes the name of the adapter command settings file, a component identifier, and notes on the adapter command settings file.

(1) Naming rule of the adapter command settings file

The following is the naming rule of the adapter command settings file:

`Adapter`*component-identifier*`.conf`

For example, if the component identifier is `/HITACHI/JP1/BASE/GETHOSTNAME`, the adapter command settings file name will be `Adapter_HITACHI_JP1_BASE_GETHOSTNAME.conf`.

(2) Component identifier

A component identifier is a string for identifying a component of each product. A specific component identifier is assigned to each component of the individual linked product.

If a product name specified by `product` in the target host definition file for configuration collection partially matches a component identifier, the Intelligent Integrated Management Base executes the adapter command plug-in of the component to collect configuration information.

`SYSTEM`, `DEFAULT`, and a string starting with `HITACHI` are reserved identifiers. Follow the rules below when creating a component identifier:

- Identifier size: Up to 240 bytes
- Available characters: ASCII numbers, uppercase alphabetic letters, and forward slash (`/`)

(3) Setting items of the adapter command settings file

For details on the settings items in the adapter command settings file, see *Table 4-4 Setting items of the adapter command settings file*.

(4) Notes on the adapter command settings file

- Even if a correct absolute path to the adapter command is not specified as the path in the `cmdpath` attribute of the adapter command settings file, the `jddcreatetree` command does not cause an error. Make sure you verify that a correct path to the adapter command is specified in the development environment before operation.
- You do not have to enclose the path in double quotation marks or other characters even if the absolute path in the `cmdpath` attribute contains any space characters.
- A single row can contain a maximum of 4,096 characters.
- If there is more than one label with the same name, an error occurs.
- If a label is omitted, an error occurs.
- If even a single error exists in the file, the file is no longer valid.
- The file is terminated with the line feed character.
- The file can contain ASCII characters only.
- When you specify a label, a white space or tab character is not allowed at the beginning of the row.
- Any row containing white space or tab characters only is ignored.

7.4 IM management node tree generation function

The IM management node tree generation function is one of the functions to get IM management node related information. IM management node related information can be obtained through the three functions of system configuration information collection, IM management node link generation, and IM management node tree generation.

The system configuration information collection function collects system configuration information of a linked product using adapter commands and plug-ins. The IM management node link generation function generates relations between configurations, based on the collected configuration information. For details, see *4.4.4(6) __createLink method*.

The following table lists and describes the input and output information of the IM management node tree generation function.

Table 7–27: Input information of the IM management node tree generation function

No.	Input information	Description
1	System configuration information	System configuration information of a linked product that was collected using adapter commands and plug-ins. The system configuration information is shown in the SID and additional information of the SID. For details on the SID, see *7.1 SID*.
2	System node definition file (`imdd_systemnode.conf`)	Definition information of the hierarchical structure consisting of the system, subsystems, and underlying given nodes.
3	Category name definition file for IM management nodes (`imdd_category_name.conf`)	Definition information of the names and display orders of categories that appear in sunburst chart format or tree format.
4	Host name definition file (`imdd_host_name.conf`)	Definition information for mapping alias names to actual host names, if a product in which an alias name can be assigned to a host name is added to the configuration of IM management nodes.

Table 7–28: Output information of the IM management node tree generation function

No.	Input information	Description
1	Tree information	Information necessary to show IM management nodes in sunburst chart format or in tree format. The IM management node tree file (`imdd_nodeTree.json`) that contains tree information is generated. The tree information is shown in the tree SID and additional information of the tree SID. For details on the SID, see *7.1 SID*.

For details on the system node definition file (`imdd_systemnode.conf`), the category name definition file for IM management nodes (`imdd_category_name.conf`), and the host name definition file (`imdd_host_name.conf`), see *System node definition file (imdd_systemnode.conf)*, *Category name definition file for IM management nodes (imdd_category_name.conf)*, and *Host name definition file (imdd_host_name.conf)* in *Chapter 2. Definition Files*.

The IM management node tree generation function has the three functions of system node generation, node generation, and tree SID conversion.

7.4.1 System node generation function

The function generates tree information from the root node to the system node, based on the system configuration information and the information in the system node definition file (`imdd_systemnode.conf`).

The following table shows the input and output information of the system node generation function.

Table 7–29: Input and output information of the system node generation function

No.	Input information / Output information		Description
1	Input information	System configuration information	System configuration information of a linked product that was collected with adapter commands and plug-ins. The system configuration information is shown in the SID and additional information of the SID. For details on the SID, see *7.1 SID*.
2		System node definition file (`imdd_systemnode.conf`)	Definition information of the hierarchical structure consisting of the system, subsystems, and underlying given nodes
3	Output information	Tree information from the root node to the system node	Information necessary to show IM management nodes in sunburst chart format or in tree format. The tree information is shown in the tree SID and additional information of the tree SID. For details on the SID, see *7.1 SID*.

The system node generation function has the system node generation function using a file and one using a plug-in. Each of the functions is described below.

- System node generation function using a file

  Based on the information on the system node contained in the system node definition file (`imdd_systemnode.conf`), the tree SID and additional information of the system node are generated. The tree SID and additional information of `All Systems` of the root node are also generated.

  The following table lists the additional information to be generated of the root node and system node.

  Table 7–30: Additional information of the root node and system node

No.	Node	Structured identifier
1	rootnode	target
2		label#
3	systemnode	target
4		resourceGroup
5		label

  # Specify `All Systems`.

- System node generation function using a plug-in

  If you create a system node other than the system node defined in the system node definition file, use the system node generation function using a plug-in to generate the tree SID and additional information of the system node.

  For example, if a product that links with JP1/IM manages something similar to the concept of the JP1/IM system and the users have already been using the product, use a plug-in to generate a system node.

The following table shows what to do on the additional information of the newly created tree SID in relation to the additional information of the tree SID already created if the tree SID of the system node created with the plug-in is the same as the one of the system node created based on the system node definition file.

Table 7–31: Action on additional information when the tree SID is duplicated

No.	Structured identifier	Action
1	target	add
2	label	`label` of the tree SID already generated takes precedence
3	resourceGroup	resourceGroup of the tree SID already generated takes precedence

7.4.2 Node generation function

The function generates tree information of all nodes under the system node of a tree, joins it with the tree information from the root node to the system node generated by the system node generation function, and generates tree information of the entire tree.

The following table shows the input and output information of the node generation function.

Table 7–32: Input and output information of the node generation function

No.	Input information / Output information		Description
1	Input information	System configuration information	System configuration information of a linked product that was collected using adapter commands and plug-ins. The system configuration information is shown in the SID and additional information of the SID. For details on the SID, see *7.1 SID*.
2		Tree information to the system node	Tree information generated by the system node generation function
3		Category name definition file for IM management nodes (`imdd_category_name.conf`)	A file that defines the names and orders of IM management node categories for management groups when data collected by the Intelligent Integrated Management Base is shown in sunburst chart format or in tree format
4		Host name definition file (`imdd_host_name.conf`)	Definition information for mapping alias names to actual host names, if a product in which an alias name can be assigned to a host name is added to the configuration of IM management nodes
5	Output information	Tree information	Information necessary to show IM management nodes in sunburst chart format or in tree format. The tree information is shown in the tree SID and additional information of the tree SID. For details on the SID, see *7.1 SID*.

The node generation function consists of the node generation function using JP1/IM and the node generation function using a plug-in. Each of the functions is described below.

- Node generation function using JP1/IM

  JP1/IM generates the tree SID and additional information of the nodes under the system node. The following table shows additional information of nodes under the system node to be generated.

Table 7–33: Additional information of nodes under the system node

No.	Structured identifier
1	target
2	resourceGroup
3	label

- Node generation function using a plug-in
  A plug-in can generate the tree SID of the entire tree. When a plug-in generates a node, use the `__createTreeNode` method. For details, see *4.4.4(3) __createTreeNode method*.

The following table shows what to do on the additional information of the newly created tree SID in relation to the additional information of the tree SID already created if the tree SID under the system node created by the plug-in is the same as the one under the system node created using JP1/IM.

Table 7–34: Action on additional information when the tree SID is duplicated

No.	Structured identifier	Action
1	target	add
2	label	`label` of the tree SID already generated takes precedence
3	resourceGroup	resourceGroup of the tree SID already generated takes precedence

(1) Default tree SID

If a node does not meet the definition of the system node and is not generated by a plug-in, the tree nodes of the object root node and objects are generated according to the following rule for creating the default tree SID:

`_ROOT_AllSystems/_SYSTEM_`*type-of-the-object-root-node*`/_`*type-of-the-object-root-node*`_`*name-of-the-object-root-node*`/_CATEGORY_`*category-of-the-object*`/_SUBCATEGORY_`*subcategory-of-the-object*`/_OBJECT_`*name-of-the-object*

The following table shows the default tree SIDs.

Table 7–35: Default tree SIDs

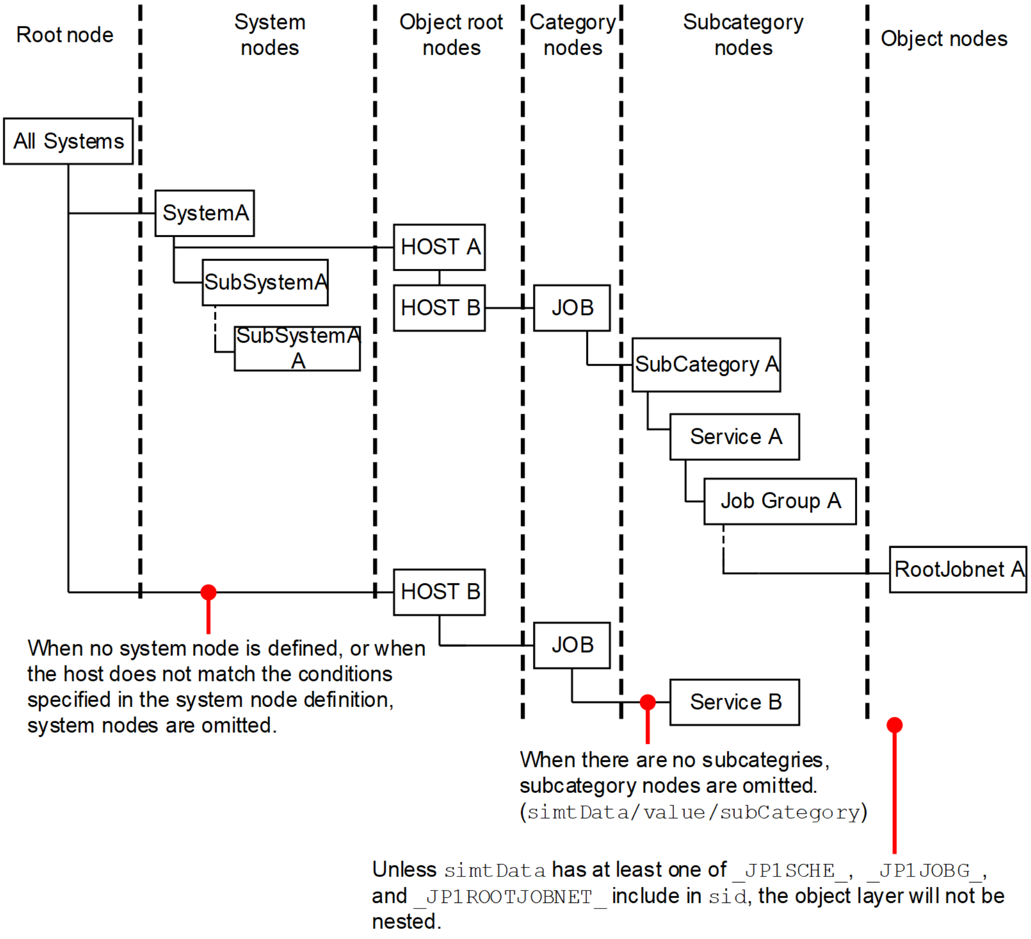
No.	IM management node type	Structured identifier name	label value	Creation condition
1	SYSTEM	Value of the `meta.objectRoot.defaultSystem.name` configuration information# Type of the object root node if the above value is not found	Value of the `meta.objectRoot.defaultSystem.label` configuration information# No value if the above value is not found	If the SID of configuration information contains the structured identifier of the object root node and `meta.objectRoot.defaultSystem`# of the configuration information is found
2	Object root node type	Name of the object root node	`label` value in the configuration information	If the SID of configuration information contains the structured identifier of the object root node
3	CATEGORY	Additional information's `category` value in the configuration information	Name resolved by the category name definition file for IM management nodes based on the additional information's	If the additional information in the configuration information has `category`

No.	IM management node type	Structured identifier name	label value	Creation condition
			`category` value in the configuration information	
4	SUBCATEGORY	Additional information's `subCategory` name in the configuration information	None	If the additional information in the configuration information has `category` and `subCategory`
5	OBJECT	Name that joins *Class* and *Name* of a structured identifier under the object root node with the SID in the configuration information	`label` value in the configuration information	If the SID of configuration information contains the structured identifier of the object root node and its subordinate structured identifier is found

#: For details on `meta.objectRoot.defaultSystem`, see *List of configuration information to be returned* in *4.4.4(1) __configurationGet method*.

The tree structure is shown in the following figure.

Figure 7–4: Tree structure



When no system node is defined, or when the host does not match the conditions specified in the system node definition, system nodes are omitted.

When there are no subcategries, subcategory nodes are omitted. (`simtData/value/subCategory`)

Unless `simtData` has at least one of `_JP1SCHE_`, `_JP1JOBG_`, and `_JP1ROOTJOBNET_` include in `sid`, the object layer will not be nested.

In the Intelligent Integrated Management Base, the tree structure is maintained in JSON format. This tree structure is referred to as a *tree object*. The following tree object depicts the tree structure shown in the figure above:

```
{
  "meta":{
    "format":"conf",
    "timestamp":"2018-11-11T11:11:11Z"
  },
  "simtData":[
    {"sid":"_ROOT_AllSystem","value":{"target":[],"label":""}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA","value":{"target":[],"resourceG
roup":["userA"],"label":"System A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA","value":{"target":[
],"label":"Host A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA/_CATEGORY_Job","valu
e":{"target":[],"label":"Job"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA/_CATEGORY_Job/_SUBCA
TEGORY_SubCategoryA","value":{"target":[],"label":""}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA/_CATEGORY_Job/_SUBCA
TEGORY_SubCategoryA/_OBJECT_ServiceA",
        "value":{"target":[],"label":"Service A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA/_CATEGORY_Job/_SUBCA
TEGORY_SubCategoryA/_OBJECT_ServiceA/_OBJECT_JobGroupA",
        "value":{"target":[],"label":"Job group A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_HOST_HostA/_CATEGORY_Job/_SUBCA
TEGORY_SubCategoryA/_OBJECT_ServiceA/_OBJECT_JobGroupA/_OBJECT_RootJobnetA",
        "value":{"target":["_JP1AJS-M_HostA/_HOST_HostA/_JP1SCHE_ServiceA/_J
P1JOBG_JobGroupA/_JP1ROOTJOBNET_RootJobnetA"],"label":"Root jobnet A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_SYSTEM_SubSystemA","value":{"ta
rget":[],"label":"Subsystem A"}},
    {"sid":"_ROOT_AllSystem/_SYSTEM_SystemA/_SYSTEM_SubSystemA/_SYSTEM_SubSy
stemAA","value":{"target":[],"label":"Subsystem AA"}},
    {"sid":"_ROOT_AllSystem/_HOST_HostB","value":{"target":["_JP1IM_IMMGR/_J
P1BASE_HostB/_HOST_HostB"],"label":"Host B"}},
    {"sid":"_ROOT_AllSystem/_HOST_HostB/_CATEGORY_Job","value":{"target":[],
"label":"Job"}},
    {"sid":"_ROOT_AllSystem/_HOST_HostB/_CATEGORY_Job/_OBJECT_ServiceB",
        "value":{"target":["_JP1IM_IMMGR/_JP1BASE_HostB/_HOST_HostB/_JP1BASE
AGT_"],"label":"Service B"}}
  ]
}
```

Tip

The order in which the simtData objects are arranged signifies the order in which the components in the same layer appear in the window.

7.4.3 Tree SID conversion function

The function retrieves SID information from collected system configuration information and the system node definition file (imdd_systemnode.conf) and converts it into the tree SID.

Multiple tree SIDs are generated depending on SID patterns of the system node definition information as input information and the definition in the system node definition file (imdd_systemnode.conf).

For details about the system node definition file (imdd_systemnode.conf), see *System node definition file (imdd_systemnode.conf)* in *Chapter 2. Definition Files*.

The following table lists tree SIDs to be generated.

Table 7–36: Tree SIDs to generated

No.	Input information		Category and subcategory information	Tree SIDs to be generated
	Definition of the system node	SID pattern		
1	Defined	The class specified in the system node definition file or `HOST` meets the class of the structured identifier at the end of the SID.	--	S1/S2/...Sn/Ax Example: `_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1`
2		The class specified in the system node definition file or `HOST` meets the class of a structured identifier that is not at the end of the SID.	With category information	• S1/S2/...Sn/Ax/C/ • S1/S2/...Sn/Ax/C/Y1 • S1/S2/...Sn/Ax/C/Y1/Y2 • S1/S2/...Sn/Ax/C/Y1/Y2 ... • S1/S2/...Sn/Ax/C/Y1/Y2/...Yn Example: `_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1/_CATEGORY_managementApplications_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1/_CATEGORY_managementApplications/_OBJECT_JP1IMMGR`
3			With category and subcategory information	• S1/S2/...Sn/Ax/C/ • S1/S2/...Sn/Ax/C/SC/Y1 • S1/S2/...Sn/Ax/C/SC/Y1/Y2 • S1/S2/...Sn/Ax/C/SC/Y1/Y2/ ... • S1/S2/...Sn/Ax/C/SC/Y1/Y2/...Yn Example: `_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1/_CATEGORY_platform_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows_ROOT_AllSystems/_SYSTEM_system1/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows/_OBJECT_TA1HOST1`
4		The class specified in the system node definition file or `HOST` does not meet the class of any structured identifier of the SID.	--	No tree SID is generated.
5	None (with the root node only)	The class specified in the system node definition file or `HOST` meets the class of the structured identifier at the end of the SID.	--	S1/Ax Example: `_ROOT_AllSystems/_HOST_HOST1`
6		The class specified in the system node definition file or `HOST` meets the	With category information	• S1/Ax/C/ • S1/Ax/C/Y1

No.	Input information		Category and subcategory information	Tree SIDs to be generated
	Definition of the system node	SID pattern		
		class of a structured identifier that is not at the end of the SID.		• S1/Ax/C/Y1/Y2 • S1/Ax/C/Y1/Y2... ... • S1/C/Y1/Y2/...Yn Example: `_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_managementApplications_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_managementApplications/_OBJECT_JP1IMMGR`
7			With category and subcategory information	• S1/Ax/C/ • S1/Ax/C/SC/Y1 • S1/Ax/C/SC/Y1/Y2 • S1/Ax/C/SC/Y1/Y2/ ... • S1/Ax/C/SC/Y1/Y2/...Yn Example: `_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows_ROOT_AllSystems/_HOST_HOST1/_CATEGORY_platform/_SUBCATEGORY_JP1%2FPFM%20-%20Windows/_OBJECT_TA1HOST1`
8		The class specified in the system node definition file or `HOST` does not meet the class of any structured identifier of the SID.	--	No tree SID is generated.

Legend:

S1/S2/...S*n*: Tree SIDs that represent the root node and the system node

A1, A2, ..., A*n*: Structured identifier

Ax: Structured identifier that contains `HOST` and object root node types

C, SC: Structured identifier that represents a category and subcategory

Y1, Y2, ..., Y*n*: Structured identifiers that represent object nodes

Important

If a host other than the host with the name specified in the system node definition file (`imdd_systemnode.conf`) or anything other than the name that corresponds to the object node type exists in the SID, it is placed under the root node, not the system node.

7.5 Sample plugin

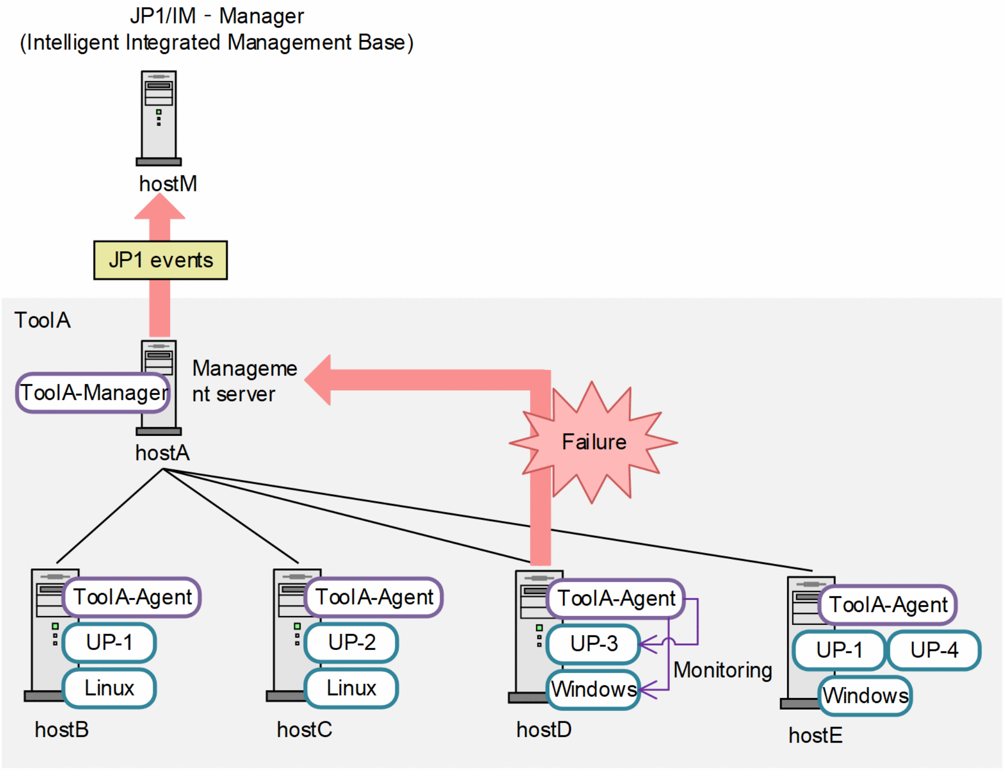
This section describes to Sample plugin.

7.5.1 Assumed operation / configuration

Manage the management tool A that monitors the Manager-Agent method with the Intelligent Integrated Management Base.

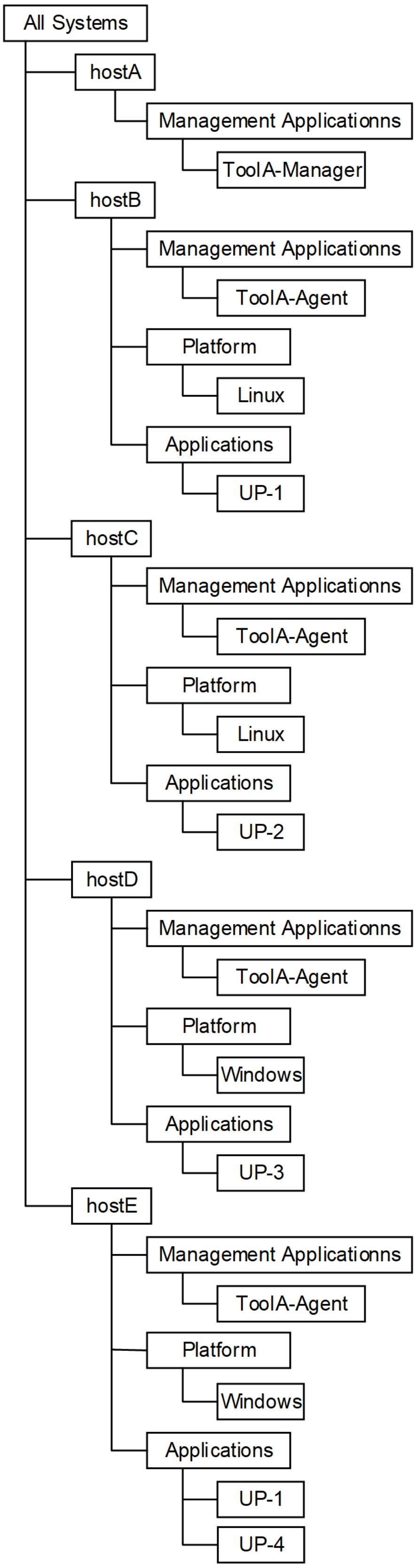
The management tool A monitors the logs and the performance of the User program / OS on the monitored host. The monitoring result is reported from an agent of the management tool A to the manager, then the manager of the management tool issues a JP1 event and notifies it to JP1/IM.

Figure 7–5: Operation and configuration using management tool A



The following figure shows the tree structure when management tool A is managed by Intelligent Integrated Management Base.

Figure 7–6: the tree structure when management tool A is managed by Intelligent Integrated Management Base



7.5.2 Example for the management node SID of the management tool A

The following table shows example SID for Manager host A and Agent host B of Management tool A.

Table 7–37: SID for Manager host A and Agent host B of Management tool A

Management host	SID	Category
ToolA-Manager Host name	_ToolA-M_hostA/_HOST_hostA	--
ToolA-Manager inside the host	_ToolA-M_hostA/_HOST_hostA/_TOOLAMGR_	Management Applications
Host name of the ToolA-Agent monitoring target host	_ToolA-M_hostA/_ToolA-A_hostB/_HOST_hostB	--
ToolA-Agr of the monitoring target host (ToolA-Agent)	_ToolA-M_hostA/_ToolA-A_hostB/ _HOST_hostB/_TOOLAAGR_	Management Applications
Platform of the monitoring target host (ToolA-Agent)	_ToolA-M_hostA/_ToolA-A_hostB/ _HOST_hostB/_PLATFORM_	Platform
User Program of the monitoring target host (ToolA-Agent)	_ToolA-M_hostA/_ToolA-A_hostB/ _HOST_hostB/_PLATFORM_UP-1	UP

7.5.3 JP1 event issued by management tool A

The following is an example of the JP1 event issued by the management tool A, for an event occurred on the Agent host D.

Table 7–38: The JP1 event issued by the management tool A, for an event occurred on the Agent host D

Event type	Event ID	B.SOURCESERVER	E.TOOLA_AGTHOST	E.UP_NAME
ToolA-Agent Event	0x7FFF8000	hostA	hostD	None
OSMonitoring Event	0x7FFF8001	hostA	hostD	None
UPMonitoring Event	0x7FFF8002	hostA	hostD	UP-3

7.5.4 Sample plugin

Following is a sample plug-in when managing the management tool A by the Intelligent Integrated Management Base.

```
/*
 * Copyright (C) 2018, Hitachi, Ltd.
 * Copyright (C) 2018, Hitachi Solutions, Ltd.
 * Licensed Material of Hitachi, Ltd.
 * Licensed Material of Hitachi Solutions, Ltd.
 */

// Component name of the management tool A
const TOOLA_COMPONENT_NAME = "/HITACHI/TOOLA";
// JavaScript name of the management tool A
const JS_NAME = "toola";
// The type of SID for representing the SID related to host
```

```
const TYPE_SID_HOST = "HOST";
// The type of SID for representing the SID related to the server of the man
agement tool A
const TYPE_SID_TOOLA_M = "ToolA-M";
// The type of SID for representing the SID related to the agent of the mana
gement tool A
const TYPE_SID_TOOLA_A = "ToolA-A";
// The type of SID for representing the SID related to the management tool
A - Manager
const TYPE_SID_TOOLA_MGR = "TOOLAMGR";
// The type of SID for representing the SID related to the management tool
A - Agent
const TYPE_SID_TOOLA_AGT = "TOOLAAGT";
// The type of SID for representing the SID related to the platform
const TYPE_SID_PLATFORM = "PLATFORM";
// The type of SID for representing the SID related to the user program
const TYPE_SID_UP = "UP";

module.exports = {

    /**
     * Convert ToolA configuration information to JSON format.
     *
     * @param {Object} args
     *     args = {
     *       hostname: string,        // Acquired host name
     *       component: string,       // Target component("/HITACHI/TOOLA")
     *       data: string,             // Result of execution of adapter com
mand(UTF-8) (except header)
     *       jp1UserName: string,     // JP1 user name
     *       jp1Token: string,        // JP1 token
     *       protocolName:string,     // Protocol name with adapter command
     *       protocolVersion:string, // Protocol version with adapter comma
nd
     *       codeset:string,          // Codeset with adapter command
     *       productName:string      // Product name with adapter command
     *       setResult:function      // Function for normal case
     *       setError:function       // Function for error case
     *     }
     */
    __configurationGet: function(args) {
        logTrace("__configurationGet start");

        if (!isValidProductName(args.component)) {
            var msg = "Componentname (" + String(args.component) + ") is inv
alid.";
            logTrace(msg);
            return;
        }

        // Configuration information object in JSON format.
        var configObj = {
            "meta": {
                "timestamp": ""
            },
            "simtData": []
        };
        try {
            // adapter command data.
            var adapterCmdDataObj = parseAdapterCmdData(args.data);

            // ToolA - Manager host name
            var mgrHostName = encodeURI(adapterCmdDataObj.hostName);

            // push SimtData for ToolA - Manager
            pushSimtDataForManagerHost(configObj.simtData, mgrHostName);

            // ToolA - Agent host object list
            var agtHostObjList = getAgentHostObjList(adapterCmdDataObj.baseU
RL, adapterCmdDataObj.uid, adapterCmdDataObj.pwd);
            agtHostObjList.forEach(function(agtHostObj) {
                // push SimtData for ToolA - Agent
                pushSimtDataForAgentHost(configObj.simtData, mgrHostName, ag
tHostObj);
            });
        } catch(e) {
            var msg = "Exception occurs. message=" + e.message;
            logTrace(msg);
            args.setError(msg);
        }

        configObj.meta.timestamp = (new Date()).toISOString();
        args.setResult(JSON.stringify(configObj));
        logTrace("__configurationGet end");
    },

    /**
     * Generate sid from JP1 event.
     *
     * @param {Object} args
     *     args = {
     *       productName: string,    // Name of the program that issued the
JP1 event.
     *       idBase: number,        // Event ID
     *       event: {value: Object}    // JP1 event attribute information
     *     }
     */
    __eventGet: function(args) {
        logTrace("__eventGet start");

        if (!isValidProductName(args.productName)) {
            return;
        }

        try {
            var sid = null;
            switch (args.idBase) {
                // generate sid of ToolA - Agent event.
                case 0x7FFF8000:
                    sid = createToolAAgtSidFromEvent(args.event.value);
                    break;

                // generate sid of os event.
                case 0x7FFF8001:
                    sid = createPlatformSidFromEvent(args.event.value);
                    break;

                // generate sid of user program event.
                case 0x7FFF8002:
                    sid = createUPSidFromEvent(args.event.value);
                    break;

                default:
                    logTrace("Unsupported args.idBase=" + args.idBase.toStri
ng(16));
                    break;
            }

            if (sid !== null) {
                logTrace("args.setTargetSid=" + sid);
                args.setTargetSid(sid);
            }

        } catch(e) {
            var msg = "Exception occurs. message=" + e.message;
            logTrace(msg);
            args.setError(msg);
        }
        logTrace("__eventGet end");
    },

    __createLink: function(args) {
        logTrace("__createLink start");

        logTrace("__createLink end");
    },

    _xxxt: function(args) {
        logTrace("_xxxt start");

        logTrace("_xxxt end");
    }
};

// if debug is true, output debug message.
var isDebug = true;

/**
 * Output log message.
 * @param {string} msg message
*/
function logTrace(msg) {
    jp1Logger.trace(JS_NAME, msg);
}

/**
 * Output log message.
 * @param {string} msg message
*/
function logDebug(msg) {
    if (!isDebug) {
        return;
    }
    jp1Logger.trace(JS_NAME, msg);
}

/**
 * Return whether product name is valid
 * @param {string} productName product name
 * @return {boolean} true if product name is valid
*/
function isValidProductName(productName) {
    return (String(productName) === TOOLA_COMPONENT_NAME);
}

/**
 * Parse data of adapter command
 * @param {string} adapterCmdData adapter command data
 * @return {Object} adapterCmdDataObj
 *     adapterCmdDataObj = {
 *       hostname: string,    // Server name
 *       baseURL: string,    // base URL for REST API
 *       uid: string,        // user id for REST API
 *       pwd: string,        // user password for REST API
 *     }
*/
function parseAdapterCmdData(adapterCmdData) {
    return JSON.parse(adapterCmdData);
}

/**
 * push simtData of ToolA - Manager
 * @param {Object[]} simtData simt data
 * @param {string} mgrHostName ToolA-Manager host name
 */
function pushSimtDataForManagerHost(simtData, mgrHostName) {
    // create Manager Host SID
    var mgrHostSid = jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, mgrHostName));
    var mgrHostSidValue = {
        component: TOOLA_COMPONENT_NAME,
        label: mgrHostName
    };
    simtData.push({
        sid: mgrHostSid,
        value: mgrHostSidValue
    });

    // create Manager SID
    var mgrSid = jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, mgrHostName),
        jp1SimtService.pack(TYPE_SID_TOOLA_MGR, ""));
    var mgrSidValue = {
        component: TOOLA_COMPONENT_NAME,
        category: "managementApplications",
        label: "ToolA - Manager"
    };
    simtData.push({
        sid: mgrSid,
        value: mgrSidValue
    });
}

/**
 * push simtData of ToolA - Agent
 * @param {Object[]} simtData simt data
 * @param {string} mgrHostName ToolA-Manager host name
 * @param {Object} agtHostObj
 */
function pushSimtDataForAgentHost(simtData, mgrHostName, agtHostObj) {
    // ToolA - Agent host name
    var agtHostName = encodeURI(agtHostObj.hostName);

    // create Agent Host SID
    var agtHostSid = jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName));
    var agtHostSidValue = {
        component: TOOLA_COMPONENT_NAME,
        label: agtHostName
    };
    simtData.push({
        sid: agtHostSid,
        value: agtHostSidValue
    });

    // create Agent SID
    var agtSid = jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
        jp1SimtService.pack(TYPE_SID_TOOLA_AGT, ""));
    var agtSidValue = {
        component: TOOLA_COMPONENT_NAME,
        category: "managementApplications",
        label: "ToolA - Agent"
    };
    simtData.push({
        sid: agtSid,
        value: agtSidValue
    });

    // create Platform SID
    var agtSid = jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
        jp1SimtService.pack(TYPE_SID_PLATFORM, ""));
    var agtSidValue = {
        component: TOOLA_COMPONENT_NAME,
        category: "platform",
        label: agtHostObj.osName
    };
    simtData.push({
        sid: agtSid,
        value: agtSidValue
    });

    // create UserProgram SID
    agtHostObj.upList.forEach(function(upName){
        var agtSid = jp1SimtService.join(
            jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
            jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
            jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
            jp1SimtService.pack(TYPE_SID_UP, upName));
        var agtSidValue = {
            component: TOOLA_COMPONENT_NAME,
            category: "up",       // custom categoryId
            label: upName
        };
        simtData.push({
            sid: agtSid,
            value: agtSidValue
        });
    });
}

/**
 * Get ToolA Agent data from ToolA - Manager
 * @param {string} baseURL ToolA-Manager host name
 * @param {string} uid userid for RESTAPI
 * @param {string} pwd password for RESTAPI
 * @return {Object[]} agtHostObjList list of agtHostObj
 *     agtHostObj = {
 *       hostName: string,    // Server name
 *       osName: string,      // OS name
 *       upList: [string]     // user program list
 *     }
 */
function getAgentHostObjList(baseURL, uid, pwd) {
    var agtHostObjList = [];

    // make url for authentication
    var fullUrl = baseURL + "/v1/authentication";
    var requestHeaderObj = {"ContentType" : "application/json"};
    var requestBody = JSON.stringify({"Username" : uid, "Password" : pwd});

    // call authentication REST API
    logTrace(fullUrl);
    logDebug(JSON.stringify(requestHeaderObj));
    logDebug(requestBody);

//    var resultObj = jp1Imdd.callRest(
//        "POST"
//        , fullUrl
//        , requestHeaderObj
//        , requestBody
//    );
//    if (resultObj.response === undefined) {
//        logTrace(JSON.stringify(resultObj));
//        return agtHostObjList;
//    }
    var resultObj = {
        "response": {
            "body": JSON.stringify({"token": "auth_token"})
        }
    };

    // authentication result
    var bodyObj = JSON.parse(resultObj.response.body);
    logDebug(JSON.stringify(bodyObj));

    // make url for agent configuration
    fullUrl = baseURL + "/v1/devices/list";
    requestHeaderObj = {"ContentType" : "application/json", "X-Authorization
" : bodyObj.token};
    requestBody = JSON.stringify({"filter": ""});

    // call agent configuration REST API
    logTrace(fullUrl);
    logDebug(JSON.stringify(requestHeaderObj));
    logDebug(requestBody);

//    resultObj = jp1Imdd.callRest(
//        "POST"
//        , fullUrl
//        , requestHeaderObj
//        , requestBody
//    );
//    if (resultObj.response === undefined) {
//        logTrace(JSON.stringify(resultObj));
//        return agtHostObjList;
//    }
    resultObj = {
        "response": {
            "body": JSON.stringify({
                "deviceList": [
                {"hostName": "hostB", "osName": "Linux", "upList": ["UP-1"]
},
                {"hostName": "hostC", "osName": "Linux", "upList": ["UP-2"]
},
                {"hostName": "hostD", "osName": "Windows", "upList": ["UP-3"
]},
                {"hostName": "hostE", "osName": "Windows", "upList": ["UP-1"
, "UP-4"]}]
            })
        }
    };

    bodyObj = JSON.parse(resultObj.response.body);
    logDebug(JSON.stringify(bodyObj));

    bodyObj.deviceList.forEach(function(deviceObj) {
        agtHostObjList.push({
            "hostName": deviceObj.hostName,
            "osName": deviceObj.osName,
            "upList": deviceObj.upList
        });
    });

    return agtHostObjList;
}
```

```
/**
 * create SID related to the ToolA - Agent from JP1 event
 * @param {Object} eventValue event value
 * @return {string} sid
*/
function createToolAAgtSidFromEvent(eventValue) {
    var mgrHostName = encodeURI(eventValue["B.SOURCESERVER"]);
    var agtHostName = encodeURI(eventValue["E.TOOLA_AGTHOST"]);

    return jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
        jp1SimtService.pack(TYPE_SID_TOOLA_AGT, ""));
}

/**
 * create SID related to the platform from JP1 event
 * @param {Object} eventValue event value
 * @return {string} sid
*/
function createPlatformSidFromEvent(eventValue) {
    var mgrHostName = encodeURI(eventValue["B.SOURCESERVER"]);
    var agtHostName = encodeURI(eventValue["E.TOOLA_AGTHOST"]);

    return jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
        jp1SimtService.pack(TYPE_SID_PLATFORM, ""));
}

/**
 * create SID related to the user program from JP1 event
 * @param {Object} eventValue event value
 * @return {string} sid
*/
function createUPSidFromEvent(eventValue) {
    var mgrHostName = encodeURI(eventValue["B.SOURCESERVER"]);
    var agtHostName = encodeURI(eventValue["E.TOOLA_AGTHOST"]);
    var upName = encodeURI(eventValue["E.UP_NAME"]);

    return jp1SimtService.join(
        jp1SimtService.packHost(TYPE_SID_TOOLA_M, mgrHostName),
        jp1SimtService.packHost(TYPE_SID_TOOLA_A, agtHostName),
        jp1SimtService.packHost(TYPE_SID_HOST, agtHostName),
        jp1SimtService.pack(TYPE_SID_UP, upName));
}
```

7.6 Control characters

The following table lists the control characters that are not available in the user-created plug-ins.

Table 7–39: Control characters that are not available in the user-created plug-ins

Code	Value	Description
00	NUL	NULl (Null)
01	SOH	Start Of Heading (Start of heading)
02	STX	Start of TeXt (Start of text)
03	ETX	End of TeXt (End of text)
04	EOT	End Of Transmission (End of transmission)
05	ENQ	ENQuiry (Inquiry)
06	ACK	ACKnowledge (Acknowledgement)
07	BEL	BELl (Bell)
08	BS	Back Space (Back space)
09	HT	Horizontal Tabulation (Horizontal tabulation)
0A	LF	Line Feed (Line feed)
0B	VT	Vertical Tabulation (Vertical tabulation)
0C	FF	Form Feed (Form feed)
0D	CR	Carriage Return (Return)
0E	SO	Shift Out (Shift Out)
0F	SI	Shift In (Shift In)
10	DLE	Data Link Escape (Extended data link control)
11	DC1	Device Control 1 (Device control 1)
12	DC2	Device Control 2 (Device control 2)
13	DC3	Device Control 3 (Device control 3)
14	DC4	Device Control 4 (Device control 4)
15	NAK	Negative AcKnowledge (Negative acknowledgement)
16	SYN	SYNchronous idle (Synchronization signal)
17	ETB	End of Transmission Block (End of transmission block)
18	CAN	CANcel (Cancel)
19	EM	End of Medium (End of medium)
1A	SUB	SUBstitute (Substitution)
1B	ESC	ESCape (Extended)
1C	FS	File Separator (File separator)
1D	GS	Group Separator (Group separator)
1E	RS	Record Separator (Record separator)

Code	Value	Description
1F	US	Unit Separator (Unit separator)
7F	DEL	DELete (Delete)
80	PAD	PADding character (Padding character)
81	HOP	High Octet Preset (High Octet Preset)
82	BPH	Break Permitted Here (Break permission)
83	NBH	No Break Here (Break prohibition)
84	IND	INDex (Index)
85	NEL	NExt Line (New line)
86	SSA	Start of Selected Area (Start of selected area)
87	ESA	End of Selected Area (End of selected area)
88	HTS	Horizontal Tabulation Set (Horizontal tabulation set)
89	HTJ	Horizontal Tabulation with Justification (Horizontal tabulation set with justification)
8A	VTS	Vertical Tabulation Set (Vertical tabulation set)
8B	PLD	Partial Line Down (Partial line down)
8C	PLU	Partial Line Up (Partial line up)
8D	RI	Reverse line feed (Previous page)
8E	SS2	Single Shift 2 (Single character shift 2)
8F	SS3	Single Shift 3 (Single character shift 3)
90	DCS	Device Control String (Device control string)
91	PU1	Private Use 1 (Private use 1)
92	PU2	Private Use 2 (Private use 2)
93	STS	Set Transmit State (Transmission state setting)
94	CCH	Cancel CHaracter (Cancel character)
95	MW	Message Waiting (Waiting for message)
96	SPA	Start of Protected Area (Start of protected area)
97	EPA	End of Protected Area (End of protected area)
98	SOS	Start Of String (Start of string)
99	SGCI	Single Graphic Character Introducer (Start of single graphic character)
9A	SCI	Single Character Introducer (Start of single character)
9B	CSI	Control Sequence Introducer (Start of control sequence)
9C	ST	String Terminator (End of string)
9D	OSC	Operating System Command (OScommand)
9E	PM	Privacy Message (Private message)
9F	APC	Application Program Command (AP command)

8 Lists of System-Monitoring Objects (for Central Scope)

This chapter describes the system-monitoring objects provided by JP1/IM.

8.1 About system-monitoring objects

System-monitoring objects are provided by the system, and the basic setting items for each product are already defined.

For details about functions related to monitoring trees and monitoring objects to be described in this chapter, and how to view tables, see *5.2 Monitoring tree* in the *JP1/Integrated Management 3 - Manager Overview and System Design Guide*. Also, for details about how to set monitoring trees or monitoring objects, see *6.3 Using the GUI to create a monitoring tree* in the *JP1/Integrated Management 3 - Manager Configuration Guide*.

8.2 List of products for which system-monitoring objects are supported

The table below lists the products for which JP1/IM - Manager provides system-monitoring objects and, for each product, indicates whether the automatic generation function is supported.

Support of the automatic generation function for products for which JP1/IM - Manager provides system-monitoring objects

Table 8–1: Products for which JP1/IM - Manager provides system-monitoring objects and the automatic generation function support status

Product name	Automatic generation function
JP1/AJS2 07-00 or later, JP1/AJS3 09-00 or later	Supported[#3]
JP1/Cm2/SSO Version 7 or Version 8[#1, #2]	Supported[#3]
JP1/Cm2/SSO 07-00 or later[#1, #2]	Supported[#3]
JP1/PFM 07-00 or later	Supported[#3]
JP1/PAM 07-00 or later	Not supported
JP1/Software Distribution 07-00 or later	Not supported
HP NNM Version 7 or Version 8[#2]	Not supported
JP1/NNMi	Not supported
JP1/IM - Central Console 07-00 or later	Supported[#3]
Cosminexus 06-00 or later	Supported[#3]
HiRDB 07-02 or later	Not supported

#1: The product name for version 7 is JP1/PFM/SSO.

#2: To use the automatic generation function, JP1/Base Version 7 or Version 8 must be installed on the host where the linked product is installed.

#3: To use the automatic generation function, JP1/Base version 07-00 or later must be installed on the host where the linked product is installed. You also need an installed copy of JP1/IM - View with the same version as JP1/IM - Manager.

8.3 System-monitoring objects for JP1/AJS

The AJS Monitoring Object and Jobnet Monitoring (AJS) system-monitoring objects are provided For JP1/AJS.

8.3.1 AJS Monitoring system-monitoring object

Table 8–2: Overview of the system-monitoring object

Item	Description	
Monitoring node type	AJS Monitoring Object	
Purpose	Monitoring of JP1/AJS itself for failures and for the jobnet execution status	
Basic information	Object name	Complete name of the jobnet (*scheduler-service-name*:/*jobnet-name*) Example: AJSROOT1:/Job_A/Order_Processing
	Host name	Host name of the manager where JP1/AJS - Manager is installed Example: host01

Table 8–3: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Jobnet warning event (AJS)	Warning	Jobnet warning event (AJS)#	Event ID (B.ID)	00004108, 00004122, 00004123
		Object ID (E.OBJECT_NAME)		Object name in the basic information
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
Jobnet error event (AJS)	Error	Jobnet error event (AJS)#	Event ID (B.ID)	00004104, 00004131, 00004142, 00004143, 00004144
		Object ID (E.OBJECT_NAME)		Object name in the basic information
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
System warning event (AJS)	Warning	System warning event (AJS)#	Event ID (B.ID)	00004154, 00004164, 00004171, 000041F1
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
System error event (AJS)	Error	System error event (AJS)#	Event ID (B.ID)	00004110, 00004130, 00004152, 00004162, 00004170, 000041F0, 000041F3
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.3.2 Jobnet Monitoring (AJS) system-monitoring object

Table 8–4: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Jobnet Monitoring(AJS)`	
Purpose	Monitoring of job execution status	
Basic information	Job execution host	Name of the host that executes the job Example: `jp1-agent`
	Event-issuing server	Name of the host where JP1/AJS - Manager is installed Example: `jp1-manager`
	Registration name	Complete name of the root jobnet (*scheduler-service-name*`:`/*root-jobnet-name*) Example: `AJSROOT1:/Job_A/Order_Processing`

Table 8–5: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Job warning event (AJS)	`Warning`	Job warning event (AJS)#	Event ID (`B.ID`)	`00004109`
		Registration name (`E.ROOT_OBJECT_NAME`)		Registration name in the basic information
		Execution host name (`E.C0`)		Job execution host in the basic information
		Event-issuing server name (`B.SOURCESERVER`)		Event-issuing server in the basic information
Job error event (AJS)	`Error`	Job error event (AJS)#	Event ID (`B.ID`)	`00004107`
		Registration name (`E.ROOT_OBJECT_NAME`)		Registration name in the basic information
		Execution host name (`E.C0`)		Job execution host in the basic information
		Event-issuing server name (`B.SOURCESERVER`)		Event-issuing server in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.4 System-monitoring objects for JP1/Cm2/SSO

The SSO Monitoring, category monitoring (SSO), and application monitoring (SSO) system-monitoring objects are provided for JP1/Cm2/SSO version 8 or earlier.

8.4.1 Settings for monitoring system-monitoring objects for JP1/Cm2/SSO version 8 or earlier

This subsection provides necessary settings for monitoring system-monitoring objects for JP1/Cm2/SSO version 8 or earlier. The following items must be set:

- Because JP1/Cm2/SSO version 8 or earlier does not issue JP1 events, you must use the JP1/Base function to convert SNMP traps (issued by JP1/Cm2/SSO for HP NNM version 7.5 or earlier) into JP1 events. During the conversion, you must use the SNMP trap conversion function of JP1/Base to set capturing of the variable binding of an SNMP trap.
- To monitor *application monitoring* (SSO), you must edit the definition file (ssoapmon.def) for JP1/Cm2/SSO version 8 or earlier so that the source name of the variable binding for an SNMP trap is captured.

8.4.2 SSO Monitoring system-monitoring object

Table 8–6: Overview of the system-monitoring object

Item	Description	
Monitoring node type	SSO Monitoring	
Purpose	Monitoring of failures in JP1/Cm2/SSO version 8 or earlier itself	
Basic information	Host name	Host name of a monitoring server where JP1/Cm2/SSO version 8 or earlier is installed Example: host01

Table 8–7: Status change conditions

Status change condition		Common condition[#1] and individual condition		
Condition name	Status	Condition		Values to be compared
System Alert event (SSO)	Alert	System Alert event (SSO)[#1]	Event ID (B.ID)	00003A80
			SNMP Object ID (E.SNMP_OID)	---.15[#2]
		Event-issuing host name (E.SNMP_VARBIND6)		Host name in the basic information
System error event (SSO)	Error	System error event (SSO)[#1]	Event ID (B.ID)	00003A80
			SNMP Object ID (E.SNMP_OID)	---.13[#2]
		Event-issuing host name (E.SNMP_VARBIND6)		Host name in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: --- is replaced with .iso.org.dod.internet.private.enterprises.hitachi.systemAP.comet.sso.0.

8.4.3 Category Monitoring (SSO) system-monitoring object

Table 8–8: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Category Monitoring (SSO)`	
Purpose	Monitoring of the resource status monitored by JP1/Cm2/SSO version 8 or earlier	
Basic information	Category name	Category name
	Event-issuing host name	Host name of a monitoring server where JP1/Cm2/SSO version 8 or earlier is installed Example: `host01`
	Host name	Host name of a server monitored by JP1/Cm2/SSO version 8 or earlier Example: `host02`

Table 8–9: Status change conditions

Status change condition		Common condition[#1] and individual condition		
Condition name	Status	Condition		Values to be compared
Resource Alert event (SSO)	`Alert`	Resource Alert event (SSO)[#1]	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---.24`[#2]
		Source name (`E.SNMP_VARBIND12`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND11`)		Event-issuing host name in the basic information
		Category name (`E.SNMP_VARBIND2`)		Category name in the basic information
Resource error event (SSO)	`Error`	Resource error event (SSO)[#1]	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---.(21|23)`[#2]
		Source name (`E.SNMP_VARBIND12`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND11`)		Event-issuing host name in the basic information
		Category name (`E.SNMP_VARBIND2`)		Category name in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: `---` is replaced with `.iso.org.dod.internet.private.enterprises.hitachi.systemAP.comet.sso.0`.

8.4.4 Application Monitoring (SSO) system-monitoring object

Table 8–10: Overview of the system-monitoring object

Item	Description
Monitoring node type	`Application Monitoring (SSO)`
Purpose	Monitoring of the application status monitored by JP1/Cm2/SSO version 8 or earlier

Item	Description	
Basic information	Event-issuing host name	Host name of a monitoring server where JP1/Cm2/SSO version 8 or earlier is installed Example: `host01`
	Application name	Name of an application monitored by JP1/Cm2/SSO version 8 or earlier Example:`JP1/PFM`
	Host name	Host name of a server whose resources are to be collected and monitored by JP1/Cm2/SSO version 8 or earlier Example: `host02`

Table 8–11: Status change conditions

Status change condition		Common condition#1 and individual condition		
Condition name	Status	Condition		Values to be compared
Application Alert event (SSO)	`Alert`	Application Alert event (SSO)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---.(109|112|115)`#2
		Source name (`E.SNMP_VARBIND3`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND2`)		Event-issuing host name in the basic information
		Application name (`E.SNMP_VARBIND1`)		Application name in the basic information
Application error event (SSO)	`Error`	Application Alert event (SSO)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---.(108|110|111|113|116|118)`#2
		Source name (`E.SNMP_VARBIND3`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND2`)		Event-issuing host name in the basic information
		Application name (`E.SNMP_VARBIND1`)		Application name in the basic information
Process monitoring failure warning event (SSO)	`Alert`	Process monitoring failure warning event (SSO)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---.304`#2
		Host name of a monitored machine (`E.SNMP_VARBIND1`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND4`)		Event-issuing host name in the basic information
Process monitoring failure error event (SSO)	`Error`	Process monitoring failure error event (SSO)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	`---`.303#2
		Host name of a monitored machine (`E.SNMP_VARBIND1`)		Host name in the basic information
		Event-issuing host name (`E.SNMP_VARBIND4`)		Event-issuing host name in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: `---` is replaced with `.iso.org.dod.internet.private.enterprises.hitachi.systemAP.comet.sso.0`.

8.5 System-monitoring objects for JP1/PFM

The `Agent Monitoring (PFM)` system-monitoring objects are provided for JP1/PFM.

8.5.1 Settings for monitoring system-monitoring objects for JP1/PFM

This subsection explains the necessary settings for monitoring system-monitoring objects for JP1/PFM. The following items must be set:

- To manage events issued by JP1/PFM - Manager, you must specify the alarm settings of JP1/PFM - Manager in such a manner that a JP1 event is issued as an action of command execution when the alarm status changes (this is because the default setting does not issue JP1/events).

8.5.2 Agent Monitoring (PFM) system-monitoring object

Table 8–12: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Agent Monitoring(PFM)`	
Purpose	Monitoring of the status of the JP1/PFM agent	
Basic information	Object ID	Service ID of the JP1/PFM agent Example: `TA1host01`
	Event-issuing server	Name of the host where JP1/PFM - Manager is installed Example: `pfm-manager`
	Host name	Name of the host where JP1/PFM - Agent is installed Example: `pfm-agent`

Table 8–13: Status change conditions

Status change condition		Common condition#1 and individual condition		
Condition name	Status	Condition		Values to be compared
Resource error event (PFM)	`Error`	Resource error event (PFM)#2	Event level (`E.SEVERITY`)	`Error`
			Product name (`E.PRODUCT_NAME`)	`/PFM/ALARM_EVENT`
		Object ID (`E.OBJECT_ID`)		Object ID in the basic information
		Name of the host where the alarm occurred (`E.JPC_AGENT`)		Host name in the basic information
		Event-issuing server name (`B.SOURCESERVER`)		Event-issuing server in the basic information
Resource warning event (PFM)	`Warning`	Resource warning event (PFM)#1	Event level (`E.SEVERITY`)	`Warning`
			Product name (`E.PRODUCT_NAME`)	`/PFM/ALARM_EVENT`

Status change condition		Common condition[#1] and individual condition	
Condition name	Status	Condition	Values to be compared
		Object ID (E.OBJECT_ID)	Object ID in the basic information
		Name of the host where the alarm occurred (E.JPC_AGENT)	Host name in the basic information
		Event-issuing server name (B.SOURCESERVER)	Event-issuing server in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: The JP1/PFM service is identified by the product ID and function ID contained in the service ID. The following services are supported:

- Service whose product ID is not P (PFM - Manager)
- Service whose function ID is A (Agent Collector)

8.6 System-monitoring objects for JP1/PAM

The `Metric Monitoring (PAM)` and `Object Monitoring (PAM)` system-monitoring objects are provided for JP1/PAM.

8.6.1 Metric Monitoring (PAM) system-monitoring object

Table 8–14: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Metric Monitoring(PAM)`	
Purpose	Monitoring of the metric status of JP1/PAM	
Basic information	Host name	Name of the host monitored by JP1/PAM Example: `host1`

Table 8–15: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Metric error event (PAM)	`Error`	Metric error event (PAM)#	Event ID (`B.ID`)	`00004602`, `00004604`, `0000460B`
		Host name (`E.PAM_HOSTNAME`)		Host name in the basic information
Metric warning event (PAM)	`Warning`	Metric warning event (PAM)#	Event ID (`B.ID`)	`00004600`, `00004603`, `00004609`
		Host name (`E.PAM_HOSTNAME`)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.6.2 Object Monitoring (PAM) system-monitoring object

Table 8–16: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Object monitoring(PAM)`	
Purpose	Monitoring of the status of objects managed by JP1/PAM	
Basic information	Host name	Name of the host monitored by JP1/PAM Example: `host1`

Table 8–17: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Object error event (PAM)	`Error`	Object error event (PAM)#	Event ID (`B.ID`)	`00004620`, `00004625`

Status change condition		Common condition# and individual condition	
Condition name	Status	Condition	Values to be compared
		Host name (E.PAM_HOSTNAME)	Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.7 System-monitoring objects for JP1/Software Distribution

The SD Monitoring and Distribution Job Monitoring (SD) system-monitoring objects are provided for JP1/Software Distribution.

8.7.1 SD Monitoring system-monitoring object

Table 8–18: Overview of the system-monitoring object

Item	Description	
Monitoring node type	SD Monitoring	
Purpose	Monitoring of JP1/Software Distribution Manager itself for failures	
Basic information	Host name	Host name of the manager where JP1/Software Distribution Manager is installed Example: host01

Table 8–19: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Critical system event (NETM/DM)	Critical	Critical system event (NETM/DM)#	Event ID (B.ID)	00010401
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.7.2 Distribution Job Monitoring (SD) system-monitoring object

Table 8–20: Overview of the system-monitoring object

Item	Description	
Monitoring node type	Distribution Job Monitoring (SD)	
Purpose	Monitoring of the execution status of distribution jobs by JP1/Software Distribution	
Basic information	Host name	Host name of the manager where JP1/Software Distribution Manager is installed Example: host01

Table 8–21: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Distribution job error event (Software Distribution)	Error	Distribution job error event (Software Distribution)#	Event ID (B.ID)	00010403
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.8 JP1/NNMi-type system-monitoring objects

The NNMi monitoring (NNMi) and node monitoring (NNMi) system-monitoring objects are provided for JP1/NNMi.

8.8.1 Settings for monitoring system-monitoring objects for JP1/NNMi

This subsection explains the settings required when monitoring JP1/NNMi-type system-monitoring objects. When monitoring NNMi incidents issued by JP1/NNMi, management incidents and SNMP traps are not differentiated.

When using NNMi monitoring (NNMi) or node monitoring (NNMi), set the extended attribute (NNMI_FAMILY_UK) for the JP1 event converted from the NNMi incident issued by JP1/IM - EG for NNMi.

If you do not set the NNMI_FAMILY_UK extended attribute, you cannot perform monitoring by using NNMi monitoring (NNMi) or node monitoring (NNMi).

For details about setting the NNMI_FAMILY_UK extended attribute and NNMI incidents, see the *Job Management Partner 1/Integrated Management 3 - Event Gateway for Network Node Manager i Description, User's Guide and Reference*.

8.8.2 NNMi Monitoring system-monitoring object

Table 8–22: Overview of the system-monitoring object

Item	Description	
Monitoring node type	NNMi Monitoring	
Purpose	Monitoring of JP1/NNMi itself for failures	
Basic information	Host name	Host name of the manager where JP1/NNMi is installed Example: host01

Table 8–23: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
System alert event (NNMi)	Alert	System alert event (NNMi)#	Event ID (B.ID)	00006100
		Name of the node where the event occurred (E.NNMI_SRC_NODE_NAME)		Host name
Critical system event (NNMi)	Critical	Critical system event (NNMi)#	Event ID (B.ID)	00006100
		Name of the node where the event occurred (E.NNMI_SRC_NODE_NAME)		Host name
System warning event (NNMi)	Warning	System warning event (NNMi)#	Event ID (B.ID)	00006100

Status change condition		Common condition# and individual condition	
Condition name	Status	Condition	Values to be compared
		Name of the node where the event occurred (`E.NNMI_SRC_NODE_NAME`)	Host name

#: This is a common condition (condition used in common by monitoring objects).

8.8.3 Node Monitoring (NNMi) system-monitoring object

Table 8–24: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Node Monitoring (NNMi)`	
Purpose	Monitoring of the status of nodes monitored by JP1/NNMi	
Basic information	Host name	Host name of the node monitored by JP1/ NNMi Example: `host01`

Table 8–25: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Network alert event (NNMi)	`Alert`	Network alert event (NNMi)#	Event ID (`B.ID`)	`00006100`
		Name of the node where the event occurred (`E.NNMI_SRC_NODE_NAME`)		Host name in the basic information
Critical network event (NNMi)	`Critical`	Critical network event (NNMi)#	Event ID (`B.ID`)	`00006100`
		Name of the node where the event occurred (`E.NNMI_SRC_NODE_NAME`)		Host name in the basic information
Network warning event (NNMi)	`Warning`	Network warning event (NNMi)#	Event ID (`B.ID`)	`00006100`
		Name of the node where the event occurred (`E.NNMI_SRC_NODE_NAME`)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.9 System-monitoring objects for HP NNM

The `NNM Monitoring` and `Node Monitoring (NNM)` system-monitoring objects are provided for HP NNM version 8 or earlier.

8.9.1 NNM Monitoring system-monitoring object

Table 8–26: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`NNM Monitoring`	
Purpose	Monitoring of HP NNM version 8 or earlier itself for failures	
Basic information	Host name	Host name of the manager where HP NNM version 8 or earlier is installed Example: `host01`

Table 8–27: Status change conditions

Status change condition		Common condition#1 and individual condition		
Condition name	Status	Condition		Values to be compared
System alert event (NNM)	`Alert`	System alert event (NNM)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	~.(`50790429|58851330|59179066|59179227|59179229|59179230|40000020`)#2
		Name of the node where the event occurred (`E.SNMP_VARBIND2`)		Host name in the basic information
Critical system event (NNM)	`Critical`	Critical system event (NNM)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	~.(`58720265|58720270|58851329|58851332|59179058|59181005|59181006|59179225|59179228|59179232|59179234|59180002|59180005|59180100|59181002|59181004|58982397|58982398|58982401|58982402|58982415|58982417|58982422|59179061|40000028|58720263`)#2
		Name of the node where the event occurred (`E.SNMP_VARBIND2`)		Host name in the basic information
System error event (NNM)	`Error`	System error event (NNM)#1	Event ID (`B.ID`)	`00003A80`
			SNMP Object ID (`E.SNMP_OID`)	~.(`58720266|59047936|59179226|59179233|`

Status change condition		Common condition[#1] and individual condition		
Condition name	Status	Condition		Values to be compared
				59179235|58982408| 58982414|50790430| 40000021)[#1]
		Name of the node where the event occurred (E.SNMP_VARBIND2)		Host name in the basic information
System warning event (NNM)	Warning	System warning event (NNM)[#1]	Event ID (B.ID)	00003A80
			SNMP Object ID (E.SNMP_OID)	~.(40000027|58982399| 59179065)[#2]
		Name of the node where the event occurred (E.SNMP_VARBIND2)		Host name in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: Replace ~ with .iso.org.dod.internet.private.enterprises.hp.nm.openView.hpOpenView.0.

8.9.2 Node Monitoring (NNM) system-monitoring object

Table 8–28: Overview of the system-monitoring object

Item	Description	
Monitoring node type	Node Monitoring(NNM)	
Purpose	Monitoring of the status of nodes monitored by HP NNM version 8 or earlier	
Basic information	Host name	Host name of the node monitored by HP NNM version 8 or earlier Example: host01

Table 8–29: Status change conditions

Status change condition		Common condition[#1] and individual condition		
Condition name	Status	Condition		Values to be compared
Critical network event (NNM)	Critical	Critical network event (NNM)[#1]	Event ID (B.ID)	00003A80
			SNMP Object ID (E.SNMP_OID)	~.58916868[#2]
		Name of the node where the event occurred (E.SNMP_VARBIND2)		Host name in the basic information
Network warning event (NNM)	Warning	Network warning event (NNM)[#1]	Event ID (B.ID)	00003A80
			SNMP Object ID (E.SNMP_OID)	~.(40000083| 40000084|40000085| 50790400|58916865)[#2]
		Name of the node where the event occurred (E.SNMP_VARBIND2)		Host name in the basic information

#1: This is a common condition (condition commonly used in monitoring objects).

#2: Replace ~ with .iso.org.dod.internet.private.enterprises.hp.nm.openView.hpOpenView.0.

8.10 System-monitoring objects for JP1/IM - Manager

The IM Monitoring system-monitoring object is provided for JP1/IM - Manager.

8.10.1 IM Monitoring system-monitoring object

Table 8–30: Overview of the system-monitoring object

Item	Description	
Monitoring node type	IM Monitoring	
Purpose	Monitoring of JP1/IM - Manager itself for failures	
Basic information	Host name	Host name of the manager where JP1/IM - Manager is installed Example: host01

Table 8–31: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
System warning event (IM)	Warning	System warning event (IM)#	Event ID (B.ID)	000020E6, 000020E7, 00003F91
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
System error event (IM)	Error	System error event (IM)#	Event ID (B.ID)	00002010, 00002011, 00002012, 00002020, 00002021, 000020A0, 000020E2, 000020E5, 000020E8, 00003F90
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.11 System-monitoring objects for Cosminexus

The `Logical Server Monitoring (Cosminexus)` and `J2EE Application Monitoring (Cosminexus)` system-monitoring objects are provided for Cosminexus.

8.11.1 Logical Server Monitoring (Cosminexus) system-monitoring object

Table 8–32: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Logical Server Monitoring(Cosminexus)`	
Purpose	Monitoring of JP1 events related to failures at the server level#	
Basic information	Domain name	Domain name of the Cosminexus server Example: `DOM001`
	Logical host name	Name of the logical host monitored by Cosminexus Example: `APSV001`

#: JP1 events whose event level is `Warning` or higher are monitored.

Table 8–33: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
Logical server emergency event (Cosminexus)	`Emergency`	Logical server emergency event (Cosminexus)#	Event ID (`B.ID`)	`00012000`, `00012080`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
Logical server alert event (Cosminexus)	`Alert`	Logical server alert event (Cosminexus)#	Event ID (`B.ID`)	`00012001`, `00012081`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
Logical server critical event (Cosminexus)	`Critical`	Logical server critical event (Cosminexus)#	Event ID (`B.ID`)	`00012002`, `00012082`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
Logical server error event (Cosminexus)	`Error`	Logical server error event (Cosminexus)#	Event ID (`B.ID`)	`00012003`, `00012083`

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
		Domain name (E.DOMAIN_NAME)		Domain name in the basic information
		Logical server name (E.LOGICAL_SERVER_NAME)		Logical host name in the basic information
Logical server warning event (Cosminexus)	Warning	Logical server warning event (Cosminexus)#	Event ID (B.ID)	00012004, 00012084
		Domain name (E.DOMAIN_NAME)		Domain name in the basic information
		Logical server name (E.LOGICAL_SERVER_NAME)		Logical host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.11.2 J2EE Application Monitoring (Cosminexus) system-monitoring object

Table 8–34: Overview of the system-monitoring object

Item	Description	
Monitoring node type	J2EE Application Monitoring(Cosminexus)	
Purpose	Monitoring of JP1 events related to failures at the application level#	
Basic information	Domain name	Domain name of the Cosminexus server Example: DOM001
	Logical host name	Name of the logical host monitored by Cosminexus Example: APSV001
	J2EE application name	Name of the J2EE application on the logical host that is monitored by Cosminexus Example: API

#: JP1 events whose event level is Warning or higher are monitored.

Table 8–35: Status change conditions

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
J2EE application emergency event (Cosminexus)	Emergency	J2EE application emergency event (Cosminexus)#	Event ID (B.ID)	00012090, 000120D0
		Domain name (E.DOMAIN_NAME)		Domain name in the basic information
		Logical server name (E.LOGICAL_SERVER_NAME)		Logical host name in the basic information
		J2EE application name (E.APPLICATION_NAME)		J2EE application name in the basic information

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
J2EE application alert event (Cosminexus)	`Alert`	J2EE application alert event (Cosminexus)#	Event ID (`B.ID`)	`00012091`, `000120D1`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
		J2EE application name (`E.APPLICATION_NAME`)		J2EE application name in the basic information
J2EE application critical event (Cosminexus)	`Critical`	J2EE application critical event (Cosminexus)#	Event ID (`B.ID`)	`00012092`, `000120D2`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
		J2EE application name (`E.APPLICATION_NAME`)		J2EE application name in the basic information
J2EE application error event (Cosminexus)	`Error`	J2EE application error event (Cosminexus)#	Event ID (`B.ID`)	`00012093`, `000120D3`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
		J2EE application name (`E.APPLICATION_NAME`)		J2EE application name in the basic information
J2EE application warning event (Cosminexus)	`Warning`	J2EE application warning event (Cosminexus)#	Event ID (`B.ID`)	`00012094`, `000120D4`
		Domain name (`E.DOMAIN_NAME`)		Domain name in the basic information
		Logical server name (`E.LOGICAL_SERVER_NAME`)		Logical host name in the basic information
		J2EE application name (`E.APPLICATION_NAME`)		J2EE application name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.12 System-monitoring objects for HiRDB

The `HiRDB Monitoring` system-monitoring objects are provided for HiRDB.

8.12.1 Settings for monitoring system-monitoring objects for HiRDB

This subsection provides necessary settings for monitoring system-monitoring objects for HiRDB. The following items must be set:

- To manage HiRDB-related events, you must specify settings in such a manner that the failure information managed by HiRDB is issued as JP1events (this is because the default setting does not issue JP1 events).

8.12.2 HiRDB Monitoring system-monitoring object

Table 8–36: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`HiRDB Monitoring`	
Purpose	Monitoring of HiRDB itself for failures	
Basic information	Host name	Name of the host where HiRDB is installed Example: `host02`
	HiRDB identifier	Identifier for identifying HiRDB Example: `PDB1`

Table 8–37: Status change conditions

Status change condition		Common condition[#] and individual condition		
Condition name	Status	Condition		Values to be compared
HiRDB emergency event	`Emergency`	HiRDB emergency event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/HiRDB`
			Event level (`E.SEVERITY`)	`Emergency`
		Event-issuing server name (`B.SOURCESERVER`)		Host name in the basic information
		Registration name (`E.ROOT_OBJECT_NAME`)		HiRDB identifier in the basic information
HiRDB alert event	`Alert`	HiRDB alert event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/HiRDB`
			Event level (`E.SEVERITY`)	`Alert`
		Event-issuing server name (`B.SOURCESERVER`)		Host name in the basic information
		Registration name (`E.ROOT_OBJECT_NAME`)		HiRDB identifier in the basic information
HiRDB critical event	`Critical`	HiRDB critical event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/HiRDB`

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
			Event level (E.SEVERITY)	Critical
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
		Registration name (E.ROOT_OBJECT_NAME)		HiRDB identifier in the basic information
HiRDB error event	Error	HiRDB error event#	Product name (E.PRODUCT_NAME)	/HITACHI/HiRDB
			Event level (E.SEVERITY)	Error
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
		Registration name (E.ROOT_OBJECT_NAME)		HiRDB identifier in the basic information
HiRDB warning event	Warning	HiRDB warning event#	Product name (E.PRODUCT_NAME)	/HITACHI/HiRDB
			Event level (E.SEVERITY)	Warning
		Event-issuing server name (B.SOURCESERVER)		Host name in the basic information
		Registration name (E.ROOT_OBJECT_NAME)		HiRDB identifier in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

8.13 System-monitoring objects for JP1/ServerConductor

The `Physical Host Monitoring (System Manager)` system-monitoring objects are provided for JP1/ServerConductor.

8.13.1 Settings for monitoring system-monitoring objects for JP1/ServerConductor

This subsection provides necessary settings for monitoring system-monitoring objects for JP1/ServerConductor. The following items must be set:

- To manage events related to a physical host managed by JP1/ServerConductor, you must set an alert detected by the manager service of JP1/ServerConductor to be issued as a JP1 event (this is because the default setting does not issue JP1 events).

8.13.2 Physical Host Monitoring (System Manager) Monitoring system-monitoring object

Table 8–38: Overview of the system-monitoring object

Item	Description	
Monitoring node type	`Physical Host Monitoring (System Manager)`	
Purpose	Monitoring of failures related to physical hosts managed by JP1/ServerConductor	
Basic information	Host name	Name of a physical host managed by System Manager Example: `host02`

Table 8–39: Status change condition

Status change condition		Common condition[#] and individual condition		
Condition name	Status	Condition		Values to be compared
Physical host emergency event	`Emergency`	Physical host emergency event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/SYSTEM_MANAGER`
			Event level (`E.SEVERITY`)	`Emergency`
		Name of a physical host managed by JP1/ServerConductor (`E.HSM_SERVER`)		Host name in the basic information
Physical host alert event	`Alert`	Physical host alert event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/SYSTEM_MANAGER`
			Event level (`E.SEVERITY`)	`Alert`
		Name of a physical host managed by JP1/ServerConductor (`E.HSM_SERVER`)		Host name in the basic information
Physical host critical event	`Critical`	Physical host critical event[#]	Product name (`E.PRODUCT_NAME`)	`/HITACHI/SYSTEM_MANAGER`

Status change condition		Common condition# and individual condition		
Condition name	Status	Condition		Values to be compared
			Event level (E.SEVERITY)	Critical
		Name of a physical host managed by JP1/ServerConductor (E.HSM_SERVER)		Host name in the basic information
Physical host error event	Error	Physical host error event#	Product name (E.PRODUCT_NAME)	/HITACHI/SYSTEM_MANAGER
			Event level (E.SEVERITY)	Error
		Name of a physical host managed by JP1/ServerConductor (E.HSM_SERVER)		Host name in the basic information
Physical host warning event	Warning	Physical host warning event#	Product name (E.PRODUCT_NAME)	/HITACHI/SYSTEM_MANAGER
			Event level (E.SEVERITY)	Warning
		Name of a physical host managed by JP1/ServerConductor (E.HSM_SERVER)		Host name in the basic information

#: This is a common condition (condition commonly used in monitoring objects).

9 Monitoring Tree Models (for Central Scope)

This chapter describes the structure of monitoring trees that are generated automatically.

9.1 Templates used to generate monitoring trees automatically

The configuration of an automatically-generated monitoring tree varies depending on the template selected in the Auto-generation - Select Configuration window. The following templates are provided by Central Console:

- Work-oriented tree template
- Server-oriented tree template

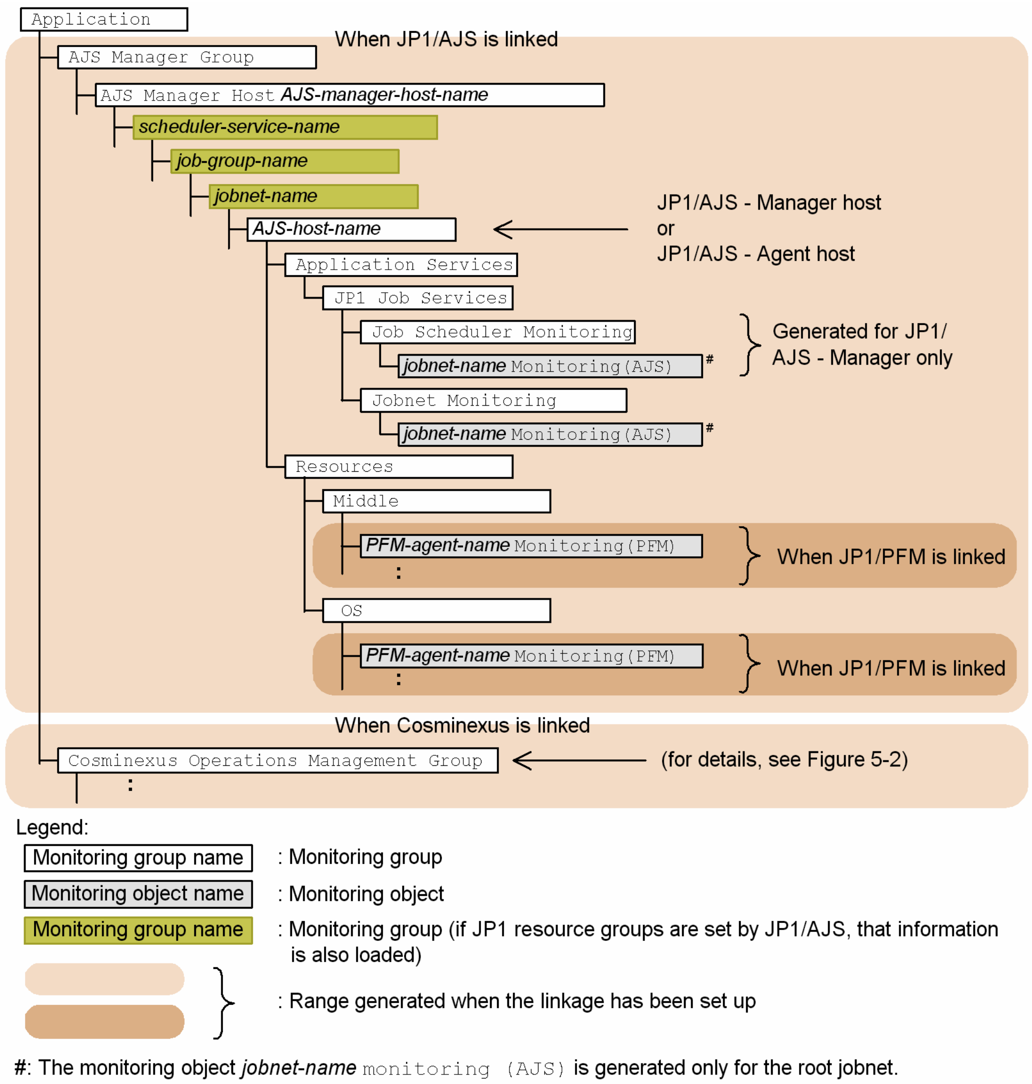
Monitoring tree models are defined for each template. Use the definitions collected from each host to generate monitoring trees automatically according to the monitoring tree model.

9.2 Monitoring tree model for the work-oriented tree

The following figures show the monitoring tree model that is generated when the work-oriented tree template is selected for generating a monitoring tree automatically.

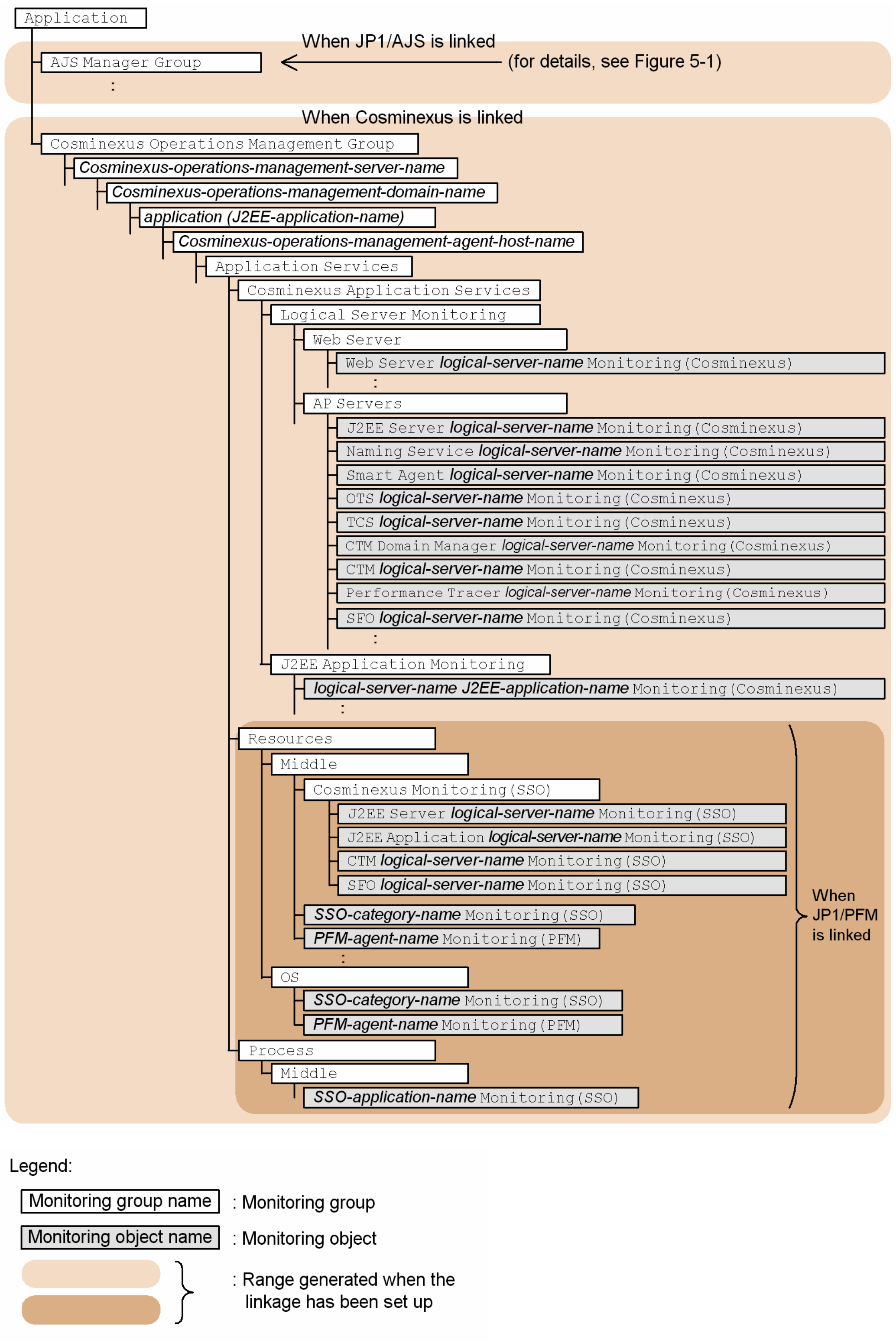
Monitoring tree model generated when the work-oriented tree template is selected

Figure 9–1: Monitoring tree model (work-oriented tree template)



#: The monitoring object *jobnet-name* monitoring (AJS) is generated only for the root jobnet.

Figure 9–2: Monitoring tree model (work-oriented tree template)


Application
When JP1/AJS is linked
AJS Manager Group
(for details, see Figure 5-1)
:
When Cosminexus is linked
Cosminexus Operations Management Group
Cosminexus-operations-management-server-name
Cosminexus-operations-management-domain-name
application (J2EE-application-name)
Cosminexus-operations-management-agent-host-name
Application Services
Cosminexus Application Services
Logical Server Monitoring
Web Server
Web Server logical-server-name Monitoring(Cosminexus)
:
AP Servers
J2EE Server logical-server-name Monitoring(Cosminexus)
Naming Service logical-server-name Monitoring(Cosminexus)
Smart Agent logical-server-name Monitoring(Cosminexus)
OTS logical-server-name Monitoring(Cosminexus)
TCS logical-server-name Monitoring(Cosminexus)
CTM Domain Manager logical-server-name Monitoring(Cosminexus)
CTM logical-server-name Monitoring(Cosminexus)
Performance Tracer logical-server-name Monitoring(Cosminexus)
SFO logical-server-name Monitoring(Cosminexus)
:
J2EE Application Monitoring
logical-server-name J2EE-application-name Monitoring(Cosminexus)
:
Resources
Middle
Cosminexus Monitoring(SSO)
J2EE Server logical-server-name Monitoring(SSO)
J2EE Application logical-server-name Monitoring(SSO)
CTM logical-server-name Monitoring(SSO)
SFO logical-server-name Monitoring(SSO)
SSO-category-name Monitoring(SSO)
PFM-agent-name Monitoring(PFM)
:
OS
SSO-category-name Monitoring(SSO)
PFM-agent-name Monitoring(PFM)
Process
Middle
SSO-application-name Monitoring(SSO)
When JP1/PFM is linked
Legend:
Monitoring group name
: Monitoring group
Monitoring object name
: Monitoring object
: Range generated when the linkage has been set up

9.3 Monitoring tree model for the server-oriented tree

The following figures show the monitoring tree model that is generated when the server-oriented tree template is selected for generating a monitoring tree automatically.

Monitoring tree model generated when the server-oriented tree template is selected

Figure 9–3: Monitoring tree model (server-oriented tree template)

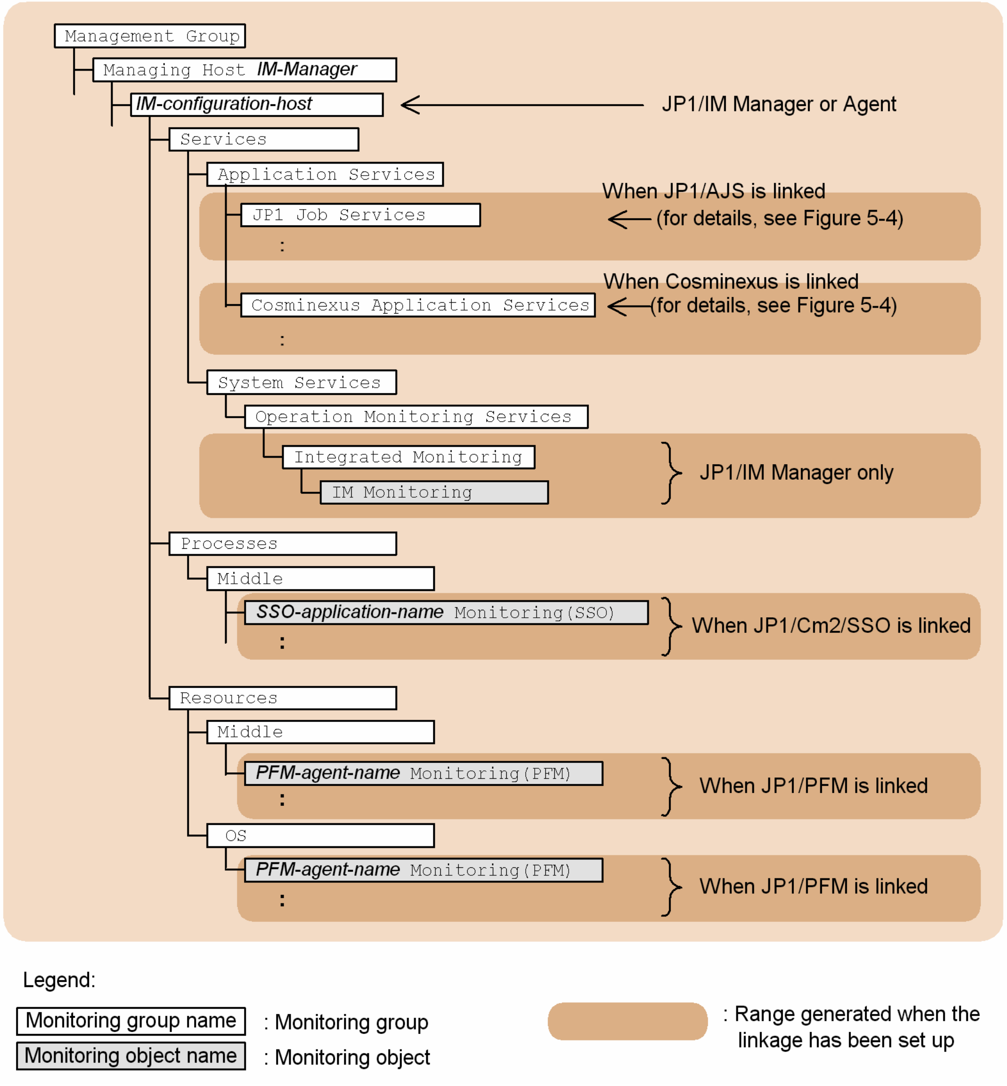
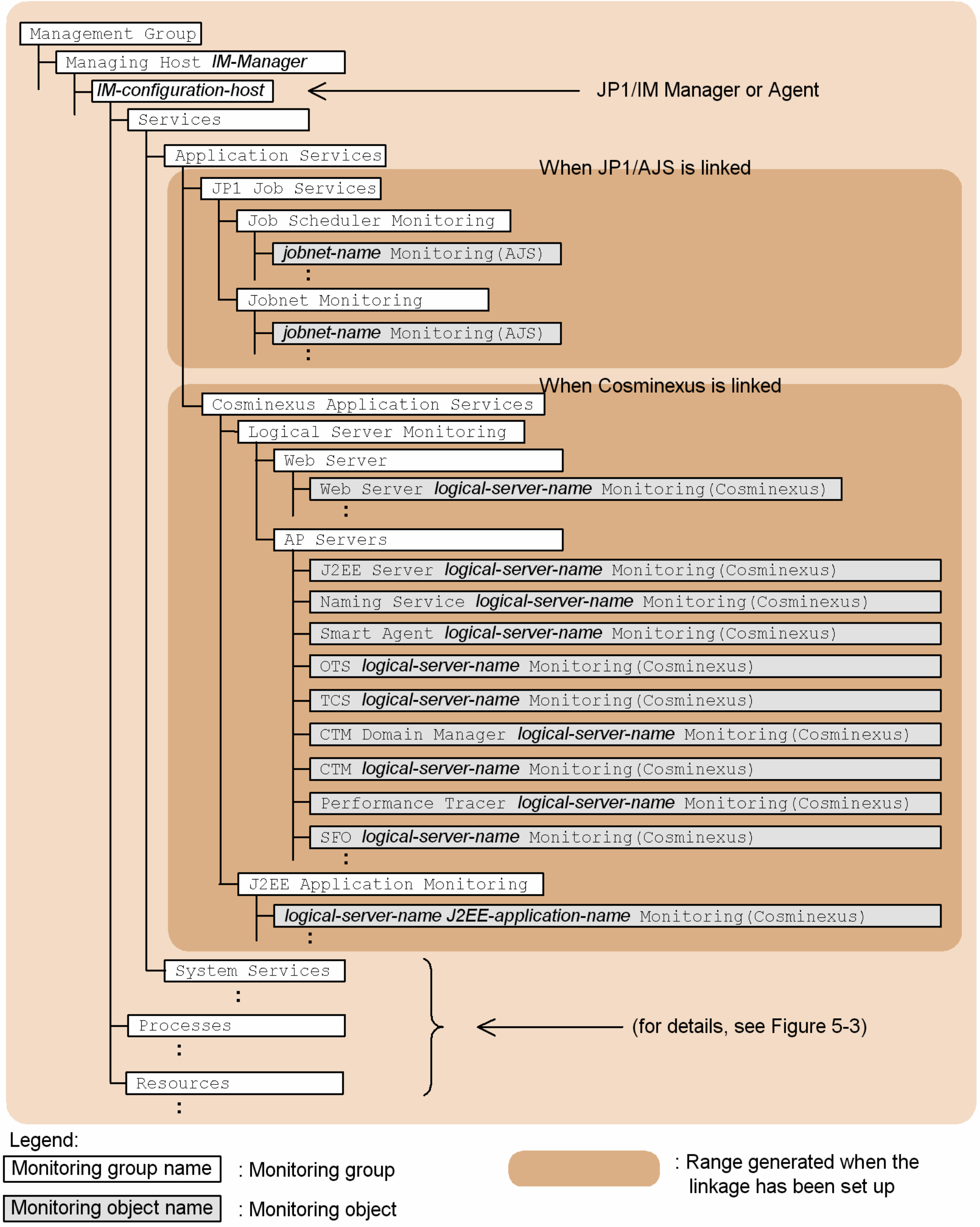


Figure 9–4: Monitoring tree model (server-oriented tree template)



Management Group
Managing Host *IM-Manager*
IM-configuration-host
JP1/IM Manager or Agent
Services
Application Services
When JP1/AJS is linked
JP1 Job Services
Job Scheduler Monitoring
jobnet-name Monitoring(AJS)
:
Jobnet Monitoring
jobnet-name Monitoring(AJS)
:
When Cosminexus is linked
Cosminexus Application Services
Logical Server Monitoring
Web Server
Web Server *logical-server-name* Monitoring(Cosminexus)
:
AP Servers
J2EE Server *logical-server-name* Monitoring(Cosminexus)
Naming Service *logical-server-name* Monitoring(Cosminexus)
Smart Agent *logical-server-name* Monitoring(Cosminexus)
OTS *logical-server-name* Monitoring(Cosminexus)
TCS *logical-server-name* Monitoring(Cosminexus)
CTM Domain Manager *logical-server-name* Monitoring(Cosminexus)
CTM *logical-server-name* Monitoring(Cosminexus)
Performance Tracer *logical-server-name* Monitoring(Cosminexus)
SFO *logical-server-name* Monitoring(Cosminexus)
:
J2EE Application Monitoring
logical-server-name J2EE-application-name Monitoring(Cosminexus)
:
System Services
:
Processes
:
Resources
:
(for details, see Figure 5-3)
Legend:
Monitoring group name
: Monitoring group
Monitoring object name
: Monitoring object
: Range generated when the linkage has been set up

Index

Hitachi, Ltd.

6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100–8280 Japan